

MS. RESEARCH THESIS

Security Enhancement and Active User Detection in 5G and B5G Wireless Networks



Submitted By

Muhammad Asif

182-FET/MSEE/S23

Supervisor: Dr. Athar Waseem

Co-Supervisor: Prof. Dr. Aqdas Naveed Malik

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

FACULTY OF ENGINEERING AND TECHNOLOGY

INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD

October, 2024

Table of Contents

List of figure	4
List of Abbreviation	5
Chapter #1 Introduction	6
1.1 5G Motivation and Vision.....	8
1.2 Key Technologies in 5G	9
1.2.1 Excellent Spectral Efficiency	10
1.2.2 Superior Energy Efficiency.....	10
1.3 Challenges in 5G and B5G Wireless Network.....	10
1.4 Problem Statement	10
1.5 Research Objectives.....	12
1.6 Main Contribution.....	13
1.6.1 Impact of contribution.....	13
1.7 Outlines of Thesis	13
Chapter # 02 Literature Review	13
2.1 Sparsity in Massive MIMO.....	18
2.1.1 Temporal Sparsity	18
2.1.2 Spatial Sparsity	18
2.1.3 Angular Sparsity	19
2.2 Compressed Sensing Based Estimation and Detection.....	20
2.2.1 Condition 1.....	20
2.2.2 Condition 2.....	21
Chapter # 03 Methodology	22
3.1 Mathematical Model	25
3.1.1 Massive MIMO scenario for AUD	26
3.2 Security Enhancement.....	27
3.2.1 Mathematical Model for Security Enhancement.....	28
3.3 OMP, MCoSaMP, MLP and GNN Algorithms	28
Chapter # 04 Simulations and Results	36
4.1 Parameters table	36
4.1.1 Compressed sensing based algorithms.....	36
4.2 Machine Learning Based Algorithms	40
4.3 OMP, MCoSaMP, MLP and GNN Comparison.....	44

4.4	Complexity Analysis.....	47
4.4.1	Complexity Analysis of OMP Vs MCoSaMP	47
4.4.2	Complexity Analysis of MLP Vs GNN	48
4.4.3	Complexity Analysis of OMP, MCoSaMP, MLP and GNN:	49
Chapter #05	Results Discussion.....	50
5.1	Channel Estimation	50
5.2	Active User Detection.....	51
5.3	Security Enhancement (Chaotic CSI)	52
5.4	Complexity Considerations.....	52
Chapter #06	Conclusion and future suggestion:.....	53
6.1	Channel Estimation:.....	53
6.2	Active User Detection:.....	53
6.3	Security Enhancement	53
Chapter #07	Reference	54

List of figure

Figure 1: Heterogeneous Network of 5G Wireless Networks [4].....	8
Figure 2: Key Technologies in 5G [8]	9
Figure 3: Massive MIMO enables spatial multiplexing. [7].....	10
Figure 4: (a) Spatial and (b) Angular Sparsity [21]	20
Figure 5: Research Methodology.....	22
Figure 6: Flow Diagram of Chanel Estimation and Active User Detection.....	23
Figure 7: Machine Learning based CE and AUD	23
Figure 8: Security Enhancement in Channel Estimation	24
Figure 9: User's connected to base station [32]	26
Figure 10: User associated with multipath component	27
Figure 11: Architecture/ block diagram of MLP.....	32
Figure 12: Block diagram of GNN	35
Figure 13: Channel Estimation for SNR range from 8-20db.....	37
Figure 14: Channel Estimation 16-QAM, SNR range 8 to 20db	38
Figure 15: Active User Detection for SNR 0 to 12db	39
Figure 16: Security Enhancement using OMP, MCoSaMP.....	39
Figure 17: Machine learning based CE, SNR range from 8 to 20db.....	41
Figure 18: Machine learning based AUD for SNR range from 0 to 12db.....	42
Figure 19: Machine learning based Security Enhancement.....	43
Figure 20: Channel Estimation using OMP, MCoSaMP, MLP and GNN.....	44
Figure 21: Channel Estimation using OMP, MCoSaMP, MLP & GNN	45
Figure 22: AUD using OMP, MCoSaMP, MLP and GNN.....	46
Figure 23: Security Enhancement using OMP, MCoSaMP, MLP and GNN	47

List of Abbreviation

IOT - Internet of thing

MIMO -Multiple input multiple output

GBPS – Giga Bits per second

GSMA – Global system for mobile communications association.

BS – Base station

UE – User Equipment

CS – compressed sensing

AUD – active user detection

DMMV- AMP – disturb multiple measurement vector approximate message passing

M2M – machine to machine

D2D – device to device

MMV – Multiple measurement vectors

SMV – single measurement vector

AMP – Approximate message passing

UMA – Unsourced multiple access

CE – Channel Estimation

LLM – Large Language Model

GANs - General Adversarial Network

LMMSE – Least minimum mean square Error.

MEC - Multi-access Edge Computing

CERTIFICATE OF APPROVAL

Title of thesis: "Security Enhancement and Active User Detection in 5G and B5G wireless network"

Name of Student: Mr. Muhammad Asif

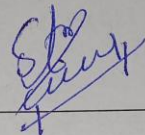
Registration No. 182-FET-MSEE-S23

Accepted by the Faculty/Department of Electrical and Computer Engineering Faculty of Engineering and Technology INTERNATIONAL ISLAMIC UNIVERSITY (IIU), ISLAMABAD, in partial fulfillment of the requirements for the Master of Science Degree in Electrical Engineering with specialization in communication System.

Viva Voce committee

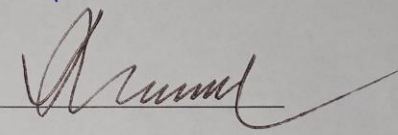
Dr. Athar Waseem (Supervisor)

Assistant Professor, DECE
FET, IIU Islamabad



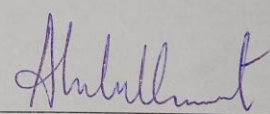
Dr. Aqdas Naveed Malik (Co-Supervisor)

Professor, DECE
FET, IIU Islamabad



Dr. Abdul Basit (Internal)

Associate Professor, DECE
FET, IIU Islamabad



Dr. Muhammad Imran (External)

Associate Professor, DEE,
Nust, Islamabad



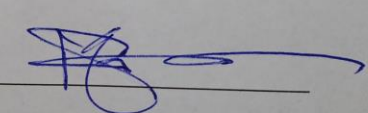
Prof. Dr. Ihsan ul Haq (Chairman, DECE)

Professor, DECE, FET, IIU Islamabad



Prof. Dr. Muhammad Amir (Dean, FET)

Professor, DECE, FET, IIU Islamabad



Chapter #1 Introduction

5G network is designed to fulfill the demand of faster speeds, lower latency and more reliable communication as compared to previous generation. Due to which massive data transformation and support technologies like IOT, AI and autonomous systems is achieved. It's faster from previous generations like 4G, 3G up to 100 times, and offer low latency in response use in application like remote surgery and automatic cars. Support large no's of devices, enabling smart cities and connected environment. Used to power advanced applications like smart cities, autonomous vehicles, remote health care treatment, internet of things, revolutionizing industries and daily life by offering enhanced connectivity and data transformations.

Massive MIMO systems use large number of antennas to simultaneously serve large number of connections or user. Basically the more antennas the better will be the performance. Massive MIMO system envision accurate beam forming and decoding with simpler linear algorithm. However efficient signal processing technique has to be used at both ends to overcome the signaling complexity. There are few fundamental issues about massive MIMO networks that needs to be better understood before their successful deployment. [1]

In order to enhance 5G technology experience regarding wireless communication devices as well as the overall technologies integrated in a whole communication systems such as automobile vehicles and Internet of things devices, many developments operations are taking place. One of the outcomes is many industrial histories that used to run in parallel, now get integrated e.g. agriculture, automotive, medical, and so on. The network infrastructure has been updated to make it more user-friendly and faster. With 5G technology acres as fast growing field and we can hope for it to assist these filed in minimum time delay which even less than one millisecond.[2]

5G comes with stronger security controls than 4G, they are better encrypted and secure in terms of privacy or authentication. Nowadays, more and more IOT devices are connecting to the 4G network and feeding our smart consumer gadgets with data from all over. 5G is not only faster and more capable; offering speeds up to 10 GBPS, but also offer high security and privacy those previous cellular generations could provide. The statement 5G is an evolution of 4G with new security protocols, entirely overlooking that existing problems have been patched. 5G itself still keeps much of the network security architecture from 4G. 5G also doesn't have the same luxury as 4G when it comes to bolting on security within network infrastructure because a significant portion of new services and technologies in combination with 5G virtualization are moving from purpose-built hardware towards software defined systems located at edge points. Hence, 5G needs more specialized security mechanisms to deal with a vast attack landscape along with many new use cases.

In [18] author provides a brief survey techniques and security protocol designed for 5G networks. Also explore advancement in encryption, authentication and data privacy measure with end to end encryption. In [19] Author introduce machine learning based approach of active user detection in massive MIMO system related to 5G and B5G, by authorization advanced signal processing and user identification techniques, proposed model improves the accuracy and reliability of user detection in crowded network environment. In [3] Author proposed a block chain integrated secure communication framework for 5G enabled IOT devices. Aim to enhance data integrity, privacy, and trust in IOT systems by addressing the growing demand in 5G network.

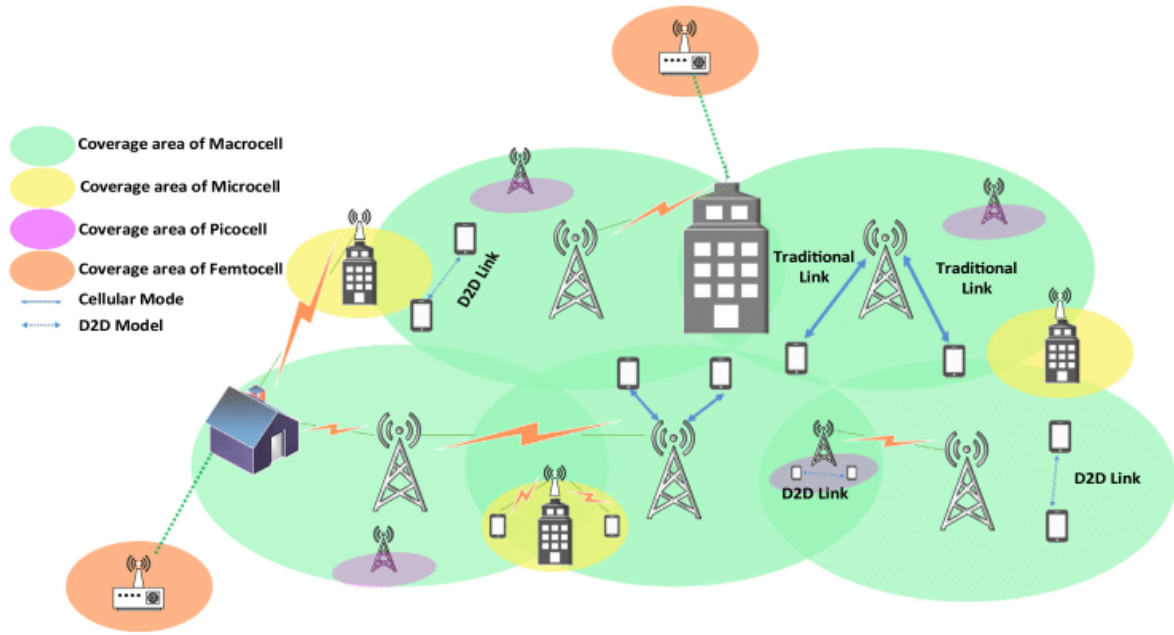


Figure 1: Heterogeneous Network of 5G Wireless Networks [4]

1.1 5G Motivation and Vision

The next fifth generation of mobile communication is triggered by the combination of new specific requirements, hyper-connected vision, and millimeter wave spectrum access. Figure 1 depicts 5G wireless communications; predict bandwidth, coverage, magnitudes of increase in data rates, wireless communication and connectivity, as well as an enormous decrease in latency and power consumption. The Group Special Mobile Association (GSMA) is working with its associates to finalize the shape of 5th generation communication. Various research initiatives from industry and academia, the major requirements of 5G have been listed below. [5] – [6]

- GBPS data rates up to 10 times higher than existing networks.
- Round trip latency as low as 1ms, nearly ten times lower than traditional 4G.

- To support massive access, 5G requires more bandwidth capacity per unit area compared to traditional values.
- The vision of IOT is to support a large number of devices; thus, it must support a large number of connected devices.
- Network availability should be close to 100%, meaning it should operate with no or very little downtime.
- Ensure maximum coverage area, it should be available in all places, regardless of the changes in users' location.
- Reducing energy demand is a key concern, with several standard organizations focusing on green technologies. To enable green technologies, it should consume 90% less energy than standard network.
- Reducing the power required to function will increase battery life.

1.2 Key Technologies in 5G

Researchers are working in numerous areas to address the major requirements of 5G technology. Massive MIMO, millimeter Wave, Small Cells, and Beam forming are the key technologies in this domain. [7]

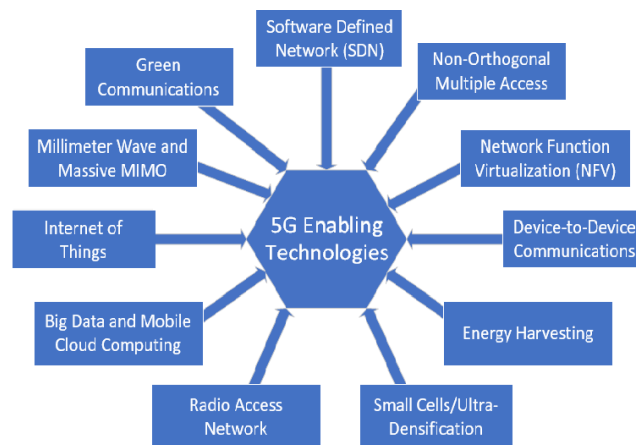


Figure 2: Key Technologies in 5G [8]

Supporting future wireless communication systems Massive MIMO is the most convincing physical-layer technology. This technique employs a large number of antennas in the pattern of an array at the BS to support a large number of autonomous user terminals, as depicted in Figure 2. To accomplish the highest capacity goal, smart processing is used at the antenna array.

1.2.1 Excellent Spectral Efficiency

Achieved by spatial multiplexing a large number of terminals on the same time-frequency resource. Efficient multiplexing necessitates channel separation between terminals, which has been demonstrated theoretically and experimentally in a variety of propagation environments. Massive MIMO, in particular, has been shown to perform equally well in line-of-sight and rich scattering.

1.2.2 Superior Energy Efficiency

In terms of array gain, this allows for a drop in radiated power. Furthermore, significant savings can be gained by applying linear processing for low precision signals. [9]

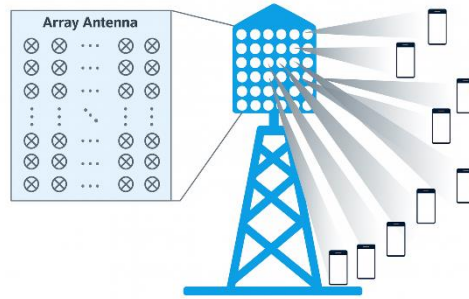


Figure 3: Massive MIMO enables spatial multiplexing. [7]

1.3 Challenges in 5G and B5G Wireless Network

The primary challenges in 5G and beyond 5G (B5G) wireless networks, especially from ethnological, architectural, and security point of view, are outlined here:

A. Spectrum Shortage and Administration:

5G relies on millimeter wave (mm Wave) and sub-6 GHz that are limited and prone to interference. B5G will need more spectrums, which may move all the way to terahertz frequency, and it will need to allocate spectrum in a wise manner and share the spectrum dynamically.

B. Extremely Low Latency and Dependability:

It is a major challenge to satisfy the requirements of highly latency (1ms or less) and reliability (99.999%) autonomous vehicles and remote surgeries among the applications. Real time environments such as packet loss, congestion and hardware limitations hinder performance.

C. Large Connectedness and Network Concentration:

5G will support up to 1 million devices per square kilometer (when it comes to highly populated IoT cases). B5G, in contrast to the previous system, has to be able to support even more densely populated environments with a limited amount of interference, which would require more efficient interference suppression and coordination of devices.

D. Security and Privacy risks:

Virtualization (SDN/NFV), scale to wide IoT, and open interfaces raise the risks of attack. Regular attacks, jamming, spoofing, DDOS, signaling disruptions, AI-powered attacks. B5G is faced with increased dangers of quantum attacks and intelligent adversaries.

E. Smart Resource Distribution:

The sophisticated process of resource allotment of bandwidth, power, and computing across ultra-dense networks dynamically. That is why the solutions based on AI/ML are under exploration, although they raise concerns related to trust, transparency.

F. Integration of Edge and Cloud:

MEC (Multi-access Edge Computing) running with cloud systems introduces the issue of latency, synchronization and reliability. In B5G, the homogeneity of the nodes of distributed computing is paramount.

G. Non-Terrestrial Networks (NTN) Incorporation:

B5G includes satellites, UAVs and high-altitude platforms, and requires effective interrelation with ground infrastructure. The barriers include coverage gaps, delays, system transfers.

H. Complexity of Network Slicing:

Network slicing is the ability to allocate specific virtual networks on shared infrastructure, which is tailored to specific applications (e.g., healthcare, smart cities). It is very challenging to maintain isolation, performance guarantees and security across slices.

I. AI/ML Reliability and Interpretability:

Despite the significant role of AI in the improvement of B5G networks, issues like bias in a model, adversarial inputs, and explainability make it problematic. Secure and easy to understand AI models are of essence.

1.4 Problem Statement

Development of the IOT and social networking with enhanced features, along with real-time video streaming for remote vehicle control and surgical performance, accelerates the growth of base stations (BSs) that provide massive data capacities for a large number of user equipment (UE) to be connected too. But for massive connectivity, existing wireless networks are unable to provide a dependable massive access. Previously, protocols for grant based and later grant-free access were introduced. In scenarios involving massive access, complex collision resolution schemes are necessary, and high access latency is noted in grant based solutions. All of the active UEs will be identified and their channels can be estimated when the base station receives data from. Scheme without allocating orthogonal channel to each UE transmitting its pilots. As UEs attempt to connect to the base station within a limited coherence time, we are aware that there are a very limited number of orthogonal channels, so this approach is ineffective. The UEs' irregular traffic is fortunately a highly significant aspect of future wireless access. There are numerous grant-free random-access schemes based on compressed sensing (CS) and machine learning (ML) that have been proposed in the literature to take advantage of this sporadic traffic property. One such scheme involves the active user detection (AUD) sparse signal recovery problem.

It has been discovered from a thorough literature review of recent advances in this field that while many authors have made extensive use of spatial sparsity and presented a great deal of work in this area, relatively little of it has made use of angular spatial sparsity. The user equipment is typically placed at a low elevation in an area with abundant local scattering that is distant from the base station, while the base station is typically located at a high elevation with few scatters nearby. In the angular domain, this results in the sparsity of massive MIMO channels. The paper will include a detailed analysis of the performance differences between angular and spatial sparsity algorithms.

1.5 Research Objectives

The main objectives of the proposed research aim to enhance the effectiveness and safety of large MIMO systems through the application of compressed sensing techniques. The research primarily aims to develop a framework utilizing compressed sensing for efficient channel estimation in extensive MIMO environments. Machine learning base models are also utilized for efficient channel estimation, active user detection and security enhancement. Secondly, it highlights the creation of ideal pilot sequences using the compressed sensing technique to improve signal accuracy and reduce overhead. Third, the research emphasizes automatic user detection (AUD) by applying compressed sensing to identify active users while conserving resources. Ultimately, the research integrates chaotic compressed sensing techniques to facilitate secure encryption, compression, and transmission of data within extensive MIMO systems.

1.6 Main Contribution

Lot of researchers are trying their best to achieved advancement in the field of wireless communication systems where they approaches to different algorithms and scenarios. In my case where we have to achieve efficient channel estimation, active user detection and security enhancement for secure communication system. For which Compressed sensing (CS) based scenarios were interpreted to obtain the efficient channel estimation, utilized active user detections and security enhancement for secure wireless network. Orthogonal matching pursuit (OMP) and Modified compressed sensing matching pursuit (MCoSaMP) were used along with 4-QAM and 16-QAM modulation. Parallel with this machine learning (ML) based scenarios were also introduced in which Multi-layer perceptron (MLP) and Graph neural network (GNN) were used to get channel estimation, active user detection and security enhancement. After this we compare both the algorithms to check which one were better and efficient.

1.6.1 Impact of contribution

Contribution lies in advancing the efficiency and reliability of wireless communication systems by addressing three critical aspects: channel estimation, active user detection, and security enhancement. The work has shown that through using compressed sensing based methods including OMP and modified CoSaMP in 4-QAM and 16-QAM modulation the technique can achieve better reconstruction and resistance to interference. Simultaneously, data-driven intelligence is introduced by the combination of machine learning models such as MLP and GNN, making the system adaptable to intricate and large-scale communication settings. The justification of the two methods shows their strengths and can be very useful in the development of secure and efficient communication networks in the future. This two-fold approach does not only enhance the theoretical knowledge of CS and ML algorithms, but also establishes a working basis of the next generation wireless systems, specifically for massive MIMO and Internet of Things.

1.7 Outlines of Thesis

A literature review presented at the second chapter of the present research compiles and analyzes the relevant findings of previous studies with specific focus on the methods, algorithms, and approaches, used in the field before. Building on the provided base, a tailored research design is developed to address the identified problem sufficiently and achieve the desired objectives. To test the proposed method, a simulation scenario is then developed to give the correct and credible results. The discussion and results section gives a comparative appraisal of the findings of this study with the findings of the previous studies giving the real advances and improvements. Finally, the conclusion

shows the key contributions of the research and provides useful recommendations to the innovation and study of wireless communication networks in the future.

Chapter # 02 Literature Review

In [10] author give a brief survey techniques and security protocol designed for 5G networks. Also explore advancement in encryption, authentication and data privacy measure with end to end encryption. In [11] Author introduce machine learning based approach of active user detection in massive MIMO system related to 5G and B5G, by authorization advanced signal processing and user identification techniques, proposed model improves the accuracy and reliability of user detection in crowded network environment.

In [3] author proposed a block chain integrated secure communication framework for 5G enabled IOT devices. Aim to enhance data integrity, privacy, and trust in IOT systems by addressing the growing demand in 5G network. In [12] author present deep learning based solution for real time active user detection in 5G network, designed to increase detection accuracy while minimizing false users by using neural networks trained on high datasets.

In [11] author offer comparative analysis of security mechanisms used in 5G and B5G networks. Review the traditional methods and compare them with the advanced/ new techniques designed for 5G network by assessing their strength, weakness and potential to handle modern security threats, gives hybrid approach by combining statically and AI techniques to detect active user detection in B5G network, to enhance the speed and precision of detection.

In [13] author discuss utilizing the intermittent traffic characteristic, the author describes a compressed sensing (CS) based random-access scheme that allows for the estimation of device channels and active devices with very little overhead for a large number of users, estimating the combined active devices and their channels in a situation that requires less overhead. Specifically, he assumes that, within the framework of compressed sensing, devices adopt pseudo-random pilots. One can design a sparse signal recovery problem for the massive access at the base station by taking advantage of the sparse nature of active devices. His distributed multiple measurement vector approximate message passing (DMMV-AMP) algorithm took advantage of the organized sparsity between the various subcarrier and receiver antennas in order to further boost performance.

In [13] author discusses Machine-to-machine (M2M) communication is a crucial technological advancement that enables data exchange between actuators and sensors in various smart city applications, such as automation, security, smart metering, surveillance, and health. Providing a suitable method for multiple users to access various devices with the least amount of overload is one of the fascinating challenges. This technique was carefully examined for its long-term evolution, and

the main problems are outlined. The security of information concerns to protect the data from unauthorized access and to safeguard its confidentiality, integrity and availability.[14]

The broadcast nature of wireless network poses various threats like eaves dropping; traffic analysis and playback message and such attacks may have increased probability in 5G and beyond network especially for D2D. Jamming is another threat which can disrupt communication totally and the spread spectrum procedures usually used as anti-jamming may not be effective in D2D networks for limited computational capacity. For security generally authentication, encryption and digital signatures are used and as such entity authentication and message authentication or both can be used. But D2D networks require robust, flexible and adaptive authentication as it has its own challenges as speed and latency necessitate special protocols.

In [15] author addresses the Random-Access Problem in Massive MIMO and redesigns the protocol, dubbed Strongest-User Collision Resolution (SUCRE). To request a dedicated pilot, UE sends an uncoordinated pilot with random access. There's a chance that another UE attempting to gain access will send the same pilot that the one sent by the UE did. The strongest candidate signal is identified in order to enable collision detection at both ends. If the UE determines that its signal at the receiving end is the strongest, it repeats the pilot. This protocol has the potential to prevent the majority of pilot collisions in populated areas.

In [16] author demonstrated how the difference in subcarrier frequency causes almost sparse common support in a massive type multiple-input/output system with large bandwidth sharing and sub-channels of orthogonal frequency division multiplexing. An optimization problem is solved to derive the learning approach for adaptive learning of the underlined structure, which improves the accuracy of channel estimation. The nearest neighbor sparsity pattern learning (AMP-NNSPL) algorithm is used for approximate message passing.

In [17] author Venture into a region with an expansive asymptotic base station, equipped with numerous antennas. Initially, it is recognized that the pilots cannot be independently distinguishable as the number of devices escalates significantly, given a confined coherence duration. In the asymptotic multi-input and multi-output domain, where there is massive access, the chances of false alarms and missed device detection for activity recognition can approach nil by utilizing compressed sensing strategies, which exploit sparsity in the pattern of user activity.

In [18] author investigates a situation in which a sizable number of devices with erratic availability are attempting to contact the base station. In this case, the primary problems are channel estimation and device detection. Because there are so many devices, they are assigned a non-orthogonal unique sequence. The principal objective of the author was to demonstrate how the combined channel

estimation and user detection problem can be formulated as a multiple measurement vector (MMV) problem or a compressed sensing single measurement vector (SMV) problem, subject to the condition that the base station has multiple or single antennas. This can be accomplished effectively by utilizing an approximate message passing (AMP) algorithm.

In [19] author for unsourced multiple access (UMA) in massive MIMO and MIMO channels, propose new receiver algorithms and transmission schemes. In the beginning, the transmitter's information is channel encoded. Following the creation of sub blocks using the coded bits, each sub-block is modulated before being transmitted. Both massive MIMO and MIMO channels use a conventional nonlinear modulation scheme, in which each block is mapped onto a transmitted signal vector. He offers a new hybrid modulation scheme for the massive MIMO channel that modulates the first sub-block nonlinearly and modulates the subsequent sub-blocks linearly before spreading them via the first sub-block signal, thereby reducing the receiver's complexity.

In [20] author suggests using compressed sensing (CS) based CE to solve the problem of IRS-aided millimeter wave massive MIMO systems. This approach takes advantage of the angular channel sparsity in large-scale arrays at mm Wave to achieve better CE with less pilot overhead. First, a downlink pilot framework was suggested for the transmission. Based on the compressed sensing theory, channels with high dimensions for base station to the user and IRS to the user can be jointly estimated. In this case, the pilot signals were designed with the prior knowledge that the line of sight dominated base station to IRS channel is known entity. Additionally, he takes advantage of an orthogonal matching pursuit algorithm by using common sparsity at difference sub carriers.

In [21] they proposed artificial intelligence (AI) framework for detection of cyber-attacks and threats including intrusion, phishing attacks etc. Machine learning classifier was integrated with real time for adaptive defense. In [22] they Investigates that how LLMs can assist non-experts in cyber security by means of cooperative activities like identifying phishing attempts. Improves the precision of decision-making and lowers the incidence of false alerts in threat assessment.

This [23] study presents a Decision Transformer model modified from reinforcement learning for real-time intrusion detection in networks. To analyze sequences of previous network states and forecasts possible attacks, making real-time decisions. In comparison to conventional models, it provides enhanced flexibility and reduced latency. It's particularly beneficial for changing network settings.

In [24] the author suggests a streamlined AI framework designed for use on edge devices that have restricted resources. By this model they integrate explainable AI methods with effective detection algorithms to recognize and analyze cyber threats instantly .To maintains a balance of transparency,

speed, and minimal computational expenses. The study focuses on the necessity for safe IoT and edge network settings.

In [25] author review how generative AI, such as GANs and LLMs ,is revolutionizing both offensive and defensive practices in cyber security. It also encompasses uses such as malware creation, automated threat testing, and sophisticated phishing identification. Writers also address ethical and security concerns regarding misuse. It serves as a roadmap on how to use generative models in ethics of cyber security.

In [26] they use methods to analyze the patterns in machine learning application to cyber security in the past decade. It also brings up important areas of research like intrusion detection, adversarial machine learning, and threat classification. The study highlights the growing role of AI in cyber security and suggests the possible directions of the further research. It comes in handy when identifying important avenues of research.

In [27] they examine the combination of AI techniques in the field of cyber security, including deep learning and anomaly detection. It determines the ability of AI to detect modern threats such as zero-day exploits and advanced persistent threats. The authors inform about the necessity to balance accuracy and computational efficiency. Examples of research indicate that corporate networks are better secured.

In [28] Internet of Things (IoT) links many devices to share data, yet its fast development causes significant privacy and security concerns because of the energy constraints and scaling problems. The paper will suggest an intrusion detection system (ML-IDS), as a machine learning system, to identify attacks on IoT networks. The UNSW-NB15 data were processed with the feature scaling (minimum to maximum normalization) and dimensionality reduction (PCA) then six supervised ML models were tested. Performance measures have been taken in terms of accuracy, precision, recall, F1, AUC, kappa and MCC. The system was based on competitive results of 99.9% and 99.97% of accuracy and MCC respectively, which was better than the existing methods.

In [29] Grant-free transmission in uplink machine-type communication (MTC) has fewer control overheads and latencies than full-band transmission, but user activity detection (UAD) and channel estimation (CE) are challenging, particularly when using short preambles. The proposed work suggests a deep learning framework UAD-CE-NN, which is grounded on compressive sensing to combine UAD and CE. The model uses preambles as well as the hidden data signals to increase the accuracy. It consists of two stages: a preamble detection network for initial UAD-CE and a data detection network to refine results. Compared with conventional methods, UAD-CE-NN achieves significantly higher accuracy. The gains are most notable when short preamble sequences are used.

In [30] 5G systems, a convolutional neural network-based channel state estimator (CNN-CSE) is proposed to extract channel information using transmit–receive pairs and pilots. Its performance is compared with BiLSTM, LSTM, LS, and MMSE estimators. CNN-CSE shows strong results with sufficient pilots but weakens under limited pilots, where BiLSTM performs best. Three loss functions and the Adam optimizer are used for evaluation. BiLSTM outperforms LSTM, CNN, LS, and MMSE in accuracy and robustness. Overall, DNN-based CSEs are promising for 5G as they handle large data, learn correlations, and generalize well.

2.1 Sparsity in Massive MIMO

Channel estimation is a major challenge in Massive MIMO. Least square approach has historically been used to estimate channels for multiple antenna arrays, but if we can learn anything from the literature, we can use LMMSE (Least Minimum Mean Square Error) to estimate channels if we know the average of the channel gain. There are numerous additional methods for processing this estimate based on various kinds of prior knowledge regarding the channel's characteristics. Therefore, understanding the different types of sparsity that can be used in the channel estimation process is crucial.

2.1.1 Temporal Sparsity

The state in which the channel's impulse response, in a multipath environment, includes one or more zeros along with the other pulses. These pulses can represent distinct paths that are non-overlapping and have time delays. This phenomenon would only arise in the millimeter wave band, where there are few reflected paths, rather than in situations where there is a large amount of scattering with many of them diffused in each other and have overlapping delays. Using the prior understanding of temporal sparsity, one can use this understanding to determine the arrival time of the pulses as well as their characteristics, such as their amplitude and phase.

In order for this to occur, a number of additional hardware-based requirements must be fulfilled. To ensure that the aliasing effect does not disrupt the pulses, the sampling rate must be high enough to resolve temporal resolution. Second, while impulse response at the receiver end may eliminate some sparsity, it should not have an impact on the channel's sparsity since it will gradually disperse the signals received.

2.1.2 Spatial Sparsity

Spatial sparsity arises when we include angular directions in the multi paths between the 10 transmitter and receiver for a subset. These angular directions can be used to estimate the channel and determine the pulses' amplitude and phase, among other characteristics. The concept of spatial

sparsity is defined by utilizing a unique correlation matrix, wherein the eigenvalues indicate the amplitude of a pulse in a particular direction. If any zeros are present in the Eigen values, it indicates that the pulse lacks amplitude in that direction.

The discussion of temporal sparsity indicates that its existence does not guarantee its use, just as spatial sparsity does not guarantee its use either. In order to differentiate between multiple directions with pulses and directions without pulses, a very large number of antennas must be present in the array in order for this to be utilized. The effect would spread out and we would get zeros in place of actual values if the beam width in channel paths was larger than the directional distance.

2.1.3 Angular Sparsity

In addition to the great distance, there is a significant elevation difference between the UEs and Base Station, which causes a variation in the quantity of scattering elements. In comparison to the BS, where they are significantly less common, the number of these elements is higher near the low-elevation UEs. Looking at the ring channel model for a user equipment (UE) that is far away from the base station (i.e., Sparsity in the angular domain is defined as $r \ll R$, where a large number of scattering elements produce a very small angular spread.

$$\tan^{-1} \frac{r}{R} \quad 1$$

Now for angular domain and for an individual channel of Massive MIMO for the k -th user and for the pilot subcarrier $\mathbf{p}$, we can say

$$\bar{\mathbf{w}}_{\mathbf{p},k} = \mathbf{A}_R^H \bar{\mathbf{h}}_{\mathbf{p},k} \quad 2$$

Where sparsity can be observed as

$$|\text{supp} \{\tilde{\mathbf{w}}_{\mathbf{p},k}\}|_c \ll M \quad 3$$

In all the wireless channels spatial propagation characteristics are the same hence the same scatters will be affecting all the sub channels [31]. This results in a sparsity pattern which is common in frequency domain.

$$\text{supp}\{\tilde{\mathbf{w}}_{1,k}\} = \text{supp}\{\tilde{\mathbf{w}}_{2,k}\} = \dots = \text{supp}\{\tilde{\mathbf{w}}_{p,k}\} \quad 4$$

In Massive MIMO, these two equations are known as structured angular-frequency sparsity. Additionally, these demonstrate the presence of clustered sparsity brought about by a reduced angular dispersion of multipath components with varying arrival angles. Channels estimation and active user detection will make use of these angular domain sparsity properties.

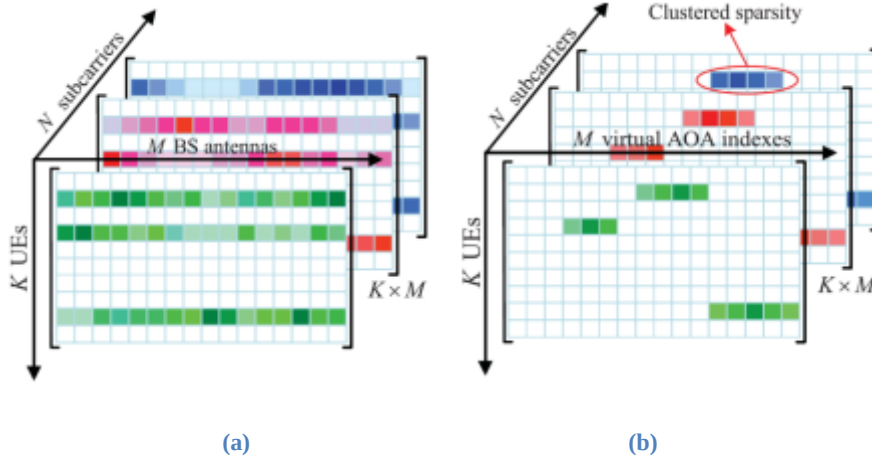


Figure 4: (a) Spatial and (b) Angular Sparsity [21]

2.2 Compressed Sensing Based Estimation and Detection

Let we have the signal of our interest which is denoted by $\mathbf{f}$ which is $n \times 1$ ($n \times m$) and it is also unknown.

We have a basis function Φ of $m \times n$. $\mathbf{f}$ is projected on basis function.

$$\mathbf{y}_{m \times 1} = \Phi_{m \times n} \mathbf{f}_{n \times 1} \quad 5$$

We need to find $\mathbf{f}$ from the knowledge of $\mathbf{f}$ and Φ . $\mathbf{f}$ Is not recoverable using linear algebra as the inverse of Φ is not possible, as it is under determinant system which solution is not possible.

For the recovery of $\mathbf{f}$ we have two conditions, which is need to be satisfied.

2.2.1 Condition 1

Sparsity: $\mathbf{f}$ should be sparse in other basis.

$$\mathbf{f} = \sum_i^N \mathbf{x}_i \Psi_j \quad 6$$

$$\mathbf{f}_{n \times 1} = \Psi_{n \times n} \mathbf{x}_{n \times 1} \quad 7$$

Ψ_j Is Matrix while $\mathbf{x}_i$ represent vector.

2.2.2 Condition 2

Incoherence; $\mathbf{f}$ should be incoherence.

$$\mu_{(\Phi, \Psi)} = \max_{i,j} | \langle \Phi_i, \Psi_j \rangle | \leq 1/\sqrt{n} \quad 8$$

$$1 \leq \mu \leq \sqrt{n} \quad 9$$

If μ approach is less than 1, then it will be incoherent, otherwise it will be coherent.

Rearrange the equations,

$$\mathbf{y} = \Phi_{m \times n} \mathbf{f}_{n \times 1} \quad 10$$

Putting the value of $\mathbf{f}_{n \times 1}$

$$\mathbf{y} = \Phi_{m \times n} \Psi_{n \times n} \mathbf{x}_{n \times 1} \quad 11$$

$$\mathbf{y} = \mathbf{A}_{m \times n} \mathbf{x}_{n \times 1} \quad 12$$

$\mathbf{A}_{m \times n}$ Transmitted Matrix in which data is store, also known as sensing Matrix. $\mathbf{x}_{n \times 1}$ Sparse vector.

Recover $\mathbf{x}_{n \times 1}$ from the knowledge of $\mathbf{y}$ and $\mathbf{A}_{m \times n}$, by using compressed sensing algorithm.

$$\min ||\hat{\mathbf{x}}||_1 \text{ such that } ||\mathbf{y} - \mathbf{A}\hat{\mathbf{x}}||_2^2 < \epsilon \quad 13$$

ϵ Is Noise / variance. If ϵ value is less $\mathbf{x}$ then algorithm will stop, otherwise it will be repeatedly going on until ϵ value become less than $\mathbf{x}$.

Chapter # 03 Methodology

The methodological research process is a carefully developed and informative channel that commences with an in-depth literature review in order to establish a strong body of information. This is then accompanied by accurate problem formulation which results in the formulation of a compressed sensing (CS) based mathematical model that describes the gist of the study. Simulation results are then used to validate the proposed model, and hence accuracy and reliability are achieved. Lastly, the work is superior and meaningful as evidenced by a critical analysis and comparison with the current strategies.

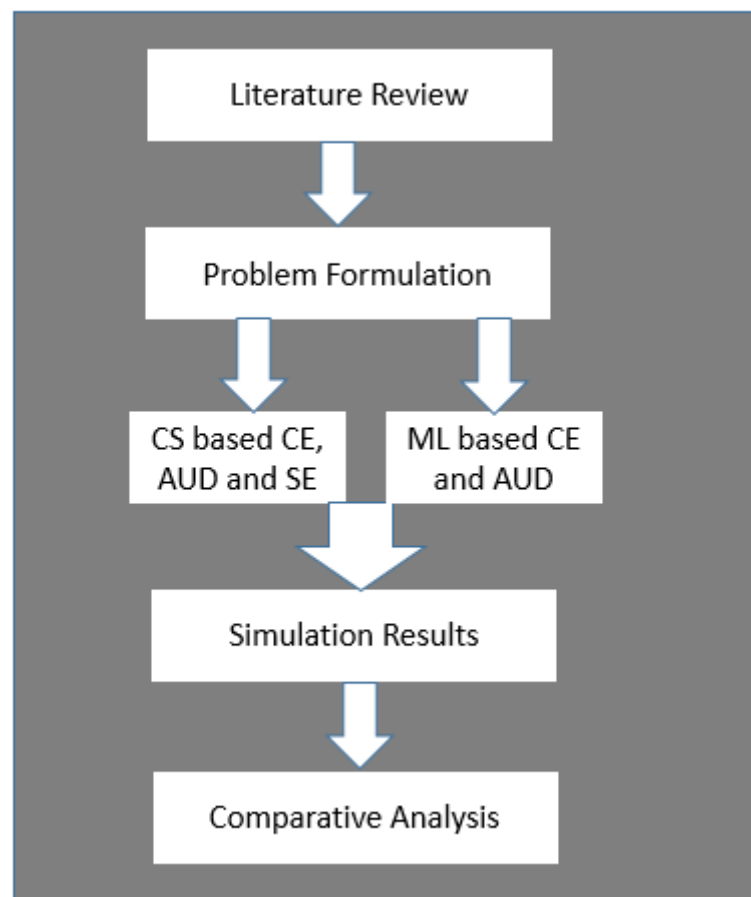


Figure 5: Research Methodology

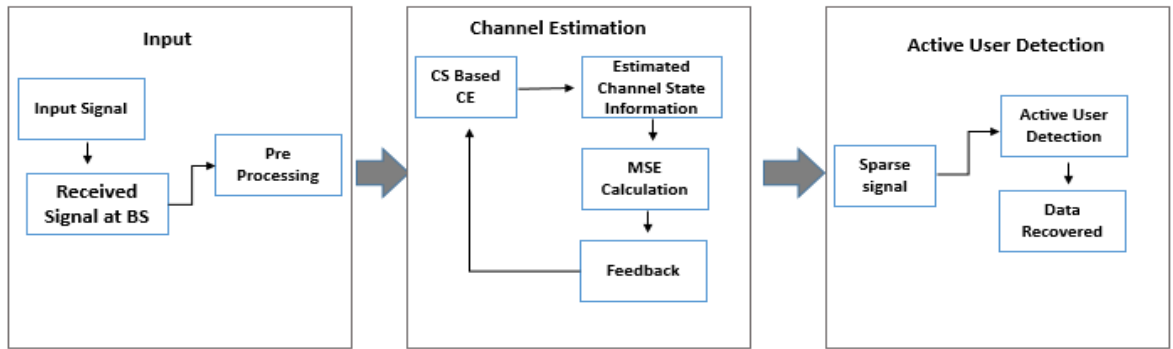


Figure 6: Flow Diagram of Chanel Estimation and Active User Detection

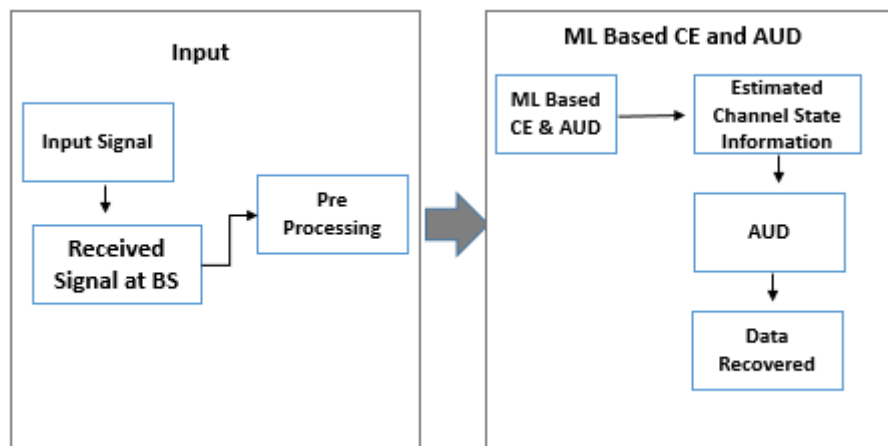


Figure 7: Machine Learning based CE and AUD

A mathematical model of uplink massive MIMO communication will be developed within the context of the compressed sensing theory, and the algorithms of the channel estimation, active user detection, and pilot distribution will be developed. In order to enhance security, an algorithm in the form of chaotic compressed sensing will be created and integrated into end-to-end communication. A critical analysis of the existing programs will be conducted in order to identify gaps and underline the need to increase security, in that regard.

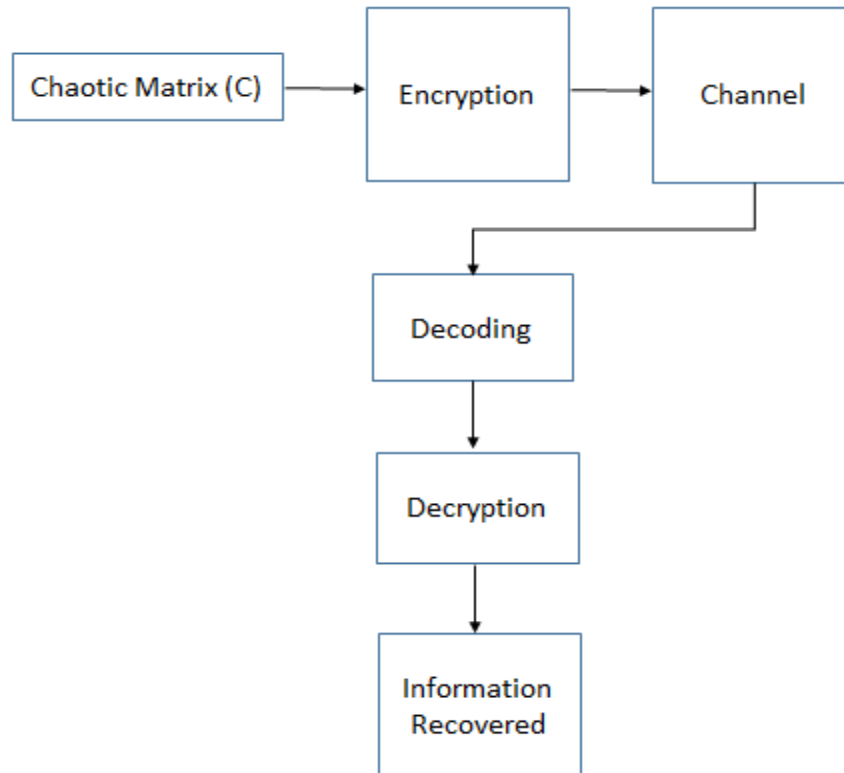


Figure 8: Security Enhancement in Channel Estimation

Mathematical modeling for the suggested schemes will be conducted, particularly focusing on the specified security requirements. An algorithm for secure compression and encryption based on chaotic CS theory will be developed, and a comprehensive, efficient, and secure framework that integrates error correction coding (ECC) with CS will be created. Machine learning based models were also introduced. The suggested models will subsequently be tested under different scenarios using Google Colab, and the results achieved will be assessed against current methods, along with a thorough complexity analysis.

3.1 Mathematical Model

We used the mathematical models to express the problems in terms of variable, parameters and functions which helps us in performance analyze and optimize solution. The general equation for channel carrier are as follow.

$$\mathbf{d}_{p,k} = \mathbf{A}_R^H \mathbf{h}_{p,k} \quad 14$$

Received signal or output is as below.

$$\mathbf{y}_{p,k}^t = \sum_{k=1}^K \alpha_k \mathbf{h}_{p,k} \mathbf{s}_{p,k}^t + \mathbf{n}_p^t \quad 15$$

Where $\mathbf{h}_{p,k} \in \mathbb{C}^{M \times 1}$ the sub channel is associated with the k-th UE, $\mathbf{s}_{p,k}^t$ is the uplink access pilot of the k-th UE, and $\mathbf{n}_p^t$ denotes the additive white Gaussian noise (AWGN) at the BS for the p-th pilot subcarrier and the t-th time slot. The UE activity indicator is denoted as α_k , and is equal to 1 when the k-th UE is active and 0 otherwise. Meanwhile, we define the set of active UEs as $A = \{k | \alpha_k = 1, 1 \leq k \leq K\}$, and the number of active UEs is denoted by $K_a = |A|_c$. Hence, the signal received at the BS from all active UEs for the p-th pilot subcarrier and the t-th time slot is given as follows.

$$\mathbf{Y}_{p,k}^t = \mathbf{H}_p \mathbf{S}_p^t + \mathbf{n}_p^t \quad 16$$

Where $\mathbf{H}_p = [\alpha_1 \mathbf{h}_{p,1}, \dots, \alpha_K \mathbf{h}_{p,K}] \in \mathbb{C}^{M \times K}$, $\mathbf{S}_p^t = [\mathbf{s}_{p,1}^t, \dots, \mathbf{s}_{p,K}^t]^T \in \mathbb{C}^{K \times 1}$.

3.1.1 Massive MIMO scenario for AUD

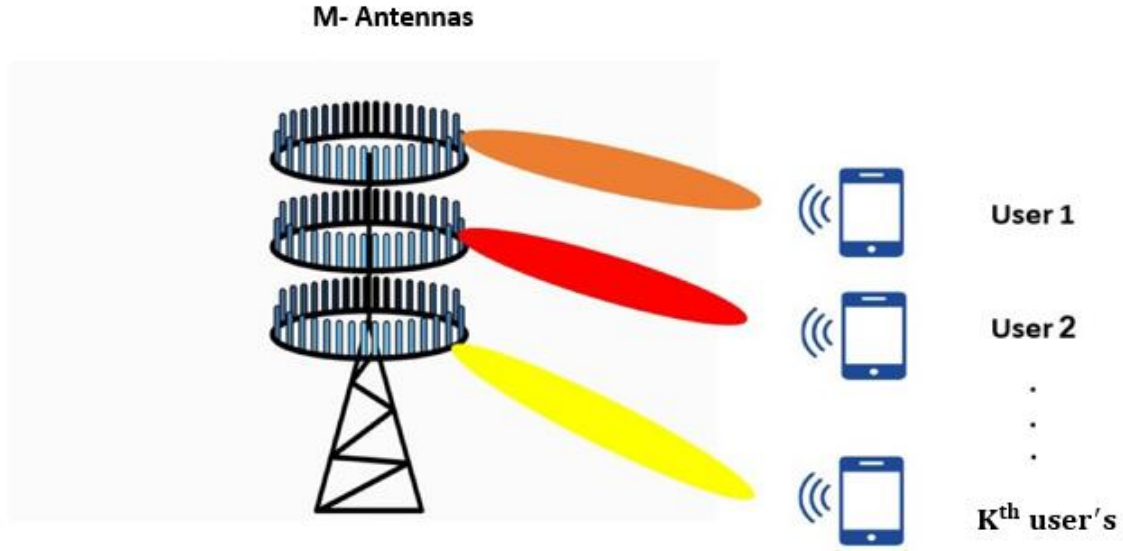


Figure 9: User's connected to base station [32]

The above figure shows the scenario of user approach to antenna for U-th user.

$$\mathbf{h}_{p,k} = \sum_1^L \beta_{k,l} \mathbf{a}_R(\Phi_{k,l}) e^{-j2\pi \bar{w}_{k,l} \left(\frac{B_s}{2} + \frac{B_s(pN/P-1)}{N} \right)} \quad 17$$

Where N/P is an integer, L denotes the number of multi-path components (MPCs), $\beta_{k,l}$ and $\bar{w}_{k,l}$ are the complex path gain and the path delay of the l -th multipath component, respectively, and B_s is the two-sided bandwidth. The array response vector $\mathbf{a}_R(\Phi_{k,l})$ is given by;

$\mathbf{a}_R(\Phi_{k,l}) = [1, e^{-2j\pi\phi_{k,l}}, \dots, e^{-2j\pi(M-1)\phi_{k,l}}]^T$, where $\phi_{k,l} = \frac{d}{\lambda} \sin(\varphi_{k,l})$. Here, $\varphi_{k,l}$ is the angle of arrival of the k -th UE's l -th multipath components, λ is the wavelength, and $d = \frac{\lambda}{2}$ is the antenna spacing.

The expansion of the above equation means there will be changed in Path gain, array factor, and path delay in correspondence to change in K , L value. If we expand the above equation up to $k=2$, it will gives us three values of multipath component ($L=2$). The above equation is expressed in the figure form given below.

It is expanded for $k=2, l=2$.

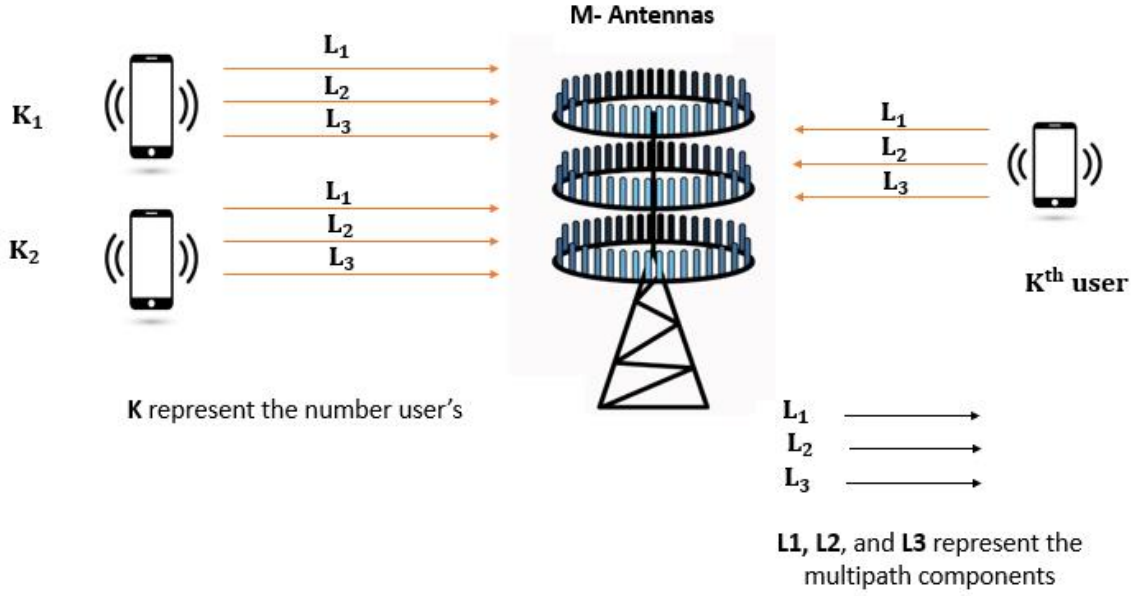


Figure 10: User associated with multipath component

3.2 Security Enhancement

Study in [33] presents an encryption method grounded in compressed sensing that utilizes generalized cascaded chaotic maps. The chaotic maps produce pseudo-random sequences utilized in data scrambling, improving both security and spectrum efficiency. The authors combine these with compressed sensing to recover sparse signals. MATLAB-based simulations show the resilience of attacks and better reconstruction accuracy in noisy settings

In [34] writer enhances positioning capabilities and radar services of 5G with the use of compressed sensing when processing Positioning Reference Signal (PRS). Orthogonal Matching Pursuit (OMP) is used to recreate the sparse radar channels, which increases resolution and detection. The method is more resistant to noise as well as more effective in object location than FFT-based methods. It makes it possible to do combined sensing and communication in 5G infrastructure.

In [35] the researcher uses compressed sensing to reconstruct wideband ISAC signals on disjoint unlicensed bands. A CS-based algorithm is highly accurate and has low complexity in identifying sparse targets. The system is a combination of spectrum sensing and radar range estimation. Signal recovery is performed using OMP and Basis Pursuit and has proven to be up to 84 times more effective than traditional signal recovery methods.

In [36] The authors develop a compressed sensing model of cooperative wideband spectrum detection in cognitive radio-enabled 5G network. They use random projection matrices and convex

maximization (Basis Pursuit) in signal reconstruction. The strategy lowers the complexity of hardware and improves energy efficiency. Simulation verifies enhanced detection capability with lowered sampling rates.

[37] Study integrates compressed sensing with deep learning to improve channel estimation and pilot decontamination in massive MIMO systems. The system employs adaptive pilot scheduling along with CS-based support detection to reduce pilot contamination. Deep neural networks enhance the limited reconstruction. Performance metrics such as BER and spectral efficiency demonstrate considerable enhancement compared to traditional approaches.

3.2.1 Mathematical Model for Security Enhancement

$\mathbf{H}_p$ Is the sub channel is associated with the k-th UE, $\mathbf{S}_p^t$ is the uplink access pilot of the k-th UE, and $\mathbf{n}_p^t$ denotes the additive white Gaussian noise (AWGN) at the BS for the p-th pilot subcarrier and the t-th time slot.

$$\mathbf{Y}_{p,k}^t = \mathbf{H}_p \mathbf{S}_p^t + \mathbf{n}_p^t \quad 18$$

The above equation is general equation for signal receiving, now we added chaotic compressed sensing part. Chaotic compressed sensing topology is used for enhancing security parameters. $\mathbf{C}_p$ Represent the chaotic sequence. $\mathbf{S}_p \rightarrow \mathbf{C}_p \times \mathbf{S}_p$ Element wise multiplication is exist between $\mathbf{C}_p$ and $\mathbf{S}_p$.

Now rearranging the above equation we get

$$\mathbf{Y}_{p,k}^t = \mathbf{H}_p (\mathbf{C}_p \times \mathbf{S}_p^t) + \mathbf{n}_p^t \quad 19$$

For matrix dimension let suppose assume $N_t = 64$ (transmit antenna at BS), $K = 500$ users, $M =$ number of pilots (i.e 8, 16, 32 etc) while p indicate the subcarrier index.

Then $\mathbf{Y}_{p,k} \in \mathbb{C}^{M \times 1}$ Received signal vector. $\mathbf{H}_p \in \mathbb{C}^{M \times N_t}$ Channel matrix (sparse). $\mathbf{S}_p \in \mathbb{C}^{N_t \times 1}$ Pilot signal for one user. $\mathbf{C}_p \in \mathbb{R}^{N_t \times 1}$ Chaotic sequence. $\mathbf{n}_p \in \mathbb{C}^{M \times 1}$ Gaussian Noise.

3.3 OMP, MCoSaMP, MLP and GNN Algorithms

The following algorithms were used in this whole scenarios, their explanation, function, roles and their working are described below.

A. OMP (Orthogonal Matching Pursuit)

Orthogonal Matching Pursuit (OMP) is a greedy compressed sensing algorithm used for signal reconstruction by iteratively selecting the column of the sensing matrix most correlated with the residual until the sparse signal is recovered. It is chosen for its low complexity compared to other CS algorithms, efficiency in sparse channel estimation for massive MIMO, and balance between accuracy and speed. In our system, OMP is applied for channel estimation, identifying active users from pilot signals, and enhancing security through chaotic CS-based signal reconstruction. The process begins with the residual equal to the received signal, then the most correlated column is added to the support set, followed by recomputing the least-squares solution, updating the residual, and repeating until a sparsity level or error threshold is reached.

$$\mathbf{y} = \Phi \mathbf{x} + \mathbf{n} \quad 20$$

Where $\mathbf{y} \in \mathbb{R}^m$ received measurement vector, $\Phi \in \mathbb{R}^{m \times n}$ is sensing (pilot) matrix, $m \ll n$, $\mathbf{x} \in \mathbb{R}^n$ original sparse signal (channel vector), and $\mathbf{n}$ is noise.

1. Initialization:

$$\mathbf{r}^0 = \mathbf{y}, \mathbf{S}^0 = \emptyset, k = 0 \quad 21$$

2. Iterations:

$$j_k = \arg \max_j | \langle \phi_j, \mathbf{r}^k \rangle | \quad 22$$

Where ϕ_j is the j -th column of Φ .

Support:

$$\mathbf{S}^{k+1} = \mathbf{S}^k \cup \{j_k\} \quad 23$$

Least Squares Estimate:

$$\hat{\mathbf{x}}^{k+1} = \arg \min_z \| \mathbf{y} - \Phi \mathbf{S}_{k+1} \mathbf{z} \|_2^2 \quad 24$$

$\Phi \mathbf{S}_{k+1}$ sub-matrix associated with selected columns.

Residual update:

$$\mathbf{r}^{k+1} = \mathbf{y} - \Phi \mathbf{S}_{k+1} \hat{\mathbf{x}}^{k+1} \quad 25$$

3. Stopping criterion:

$$\|\mathbf{r}^{k+1}\|_2 < \epsilon \text{ (Noise) or } k=K \text{ (sparsity level)}.$$

Generally it will become $\hat{\mathbf{x}} = \hat{\mathbf{x}}^k$.

B. MCoSaMP (Modified Compressive Sampling Matching Pursuit)

CoSaMP is an improved version of the MCoSaMP which is intended to solve instability and slow convergence through better support pruning, adaptive noise thresholding and faster convergence. It is preferred to OMP due to its strength in noisy conditions, superior behavior in crowded user conditions and smoother MSE behavior in channel estimation. MCoSaMP reduces reconstruction error in our system, which can be used to improve channel estimation, enables more accurate active user detection, and enhances security by resisting chaotic signal misdetection. It is started with an initial residual, using big correlation indexes, combines them with previous support, eliminates insignificant coefficients, solves least-squares on the refined support, updates the residual, and repeats until the error is minimized.

$$\mathbf{y} = \Phi \mathbf{x} + \mathbf{n} \quad 26$$

In the case where $\mathbf{y} \in \mathbb{R}^m$ was measured in, $\Phi \in \mathbb{R}^{m \times n}$ is sensing (pilot) matrix, $m \ll n$, $\mathbf{x} \in \mathbb{R}^n$ original sparse single (channel vector), and $\mathbf{n}$ is noise.

1. Initialization:

$$\mathbf{r}^0 = \mathbf{y}, \mathbf{S}^0 = \emptyset, k = 0 \quad 27$$

2. Iterations: signal proxy.

$$\mathbf{u}^k = \Phi^T \mathbf{r}^k \quad 28$$

Identification of support: Pick $2K$ largest magnitude indices.

$$\Omega^k = \text{supp} (\text{Top}_{2K}(|u^k|)) \quad 29$$

Support merge:

$$T^k = S^k \cup \Omega^k \quad 30$$

Least square Estimation:

$$b^k = \arg \min_z \|y - \Phi_{T^k} z\|_2^2 \quad 31$$

The modified step is known as support pruning:

Store best K (adaptive thresholding noise).

$$S^{k+1} = \text{supp}(\text{Top}_K(|b^k|)) \quad 32$$

Signal update

$$x_{S^{k+1}}^{k+1} = b_{S^{k+1}}^k, x_{(S^{k+1})^c}^{k+1} = 0 \quad 33$$

Residual update

$$r^{k+1} = y - \Phi x^{k+1} \quad 34$$

3. Stopping criteria

$\|r^{k+1}\|_2 < \epsilon$ Or maximum criteria reached. Final estimate will be like this $\hat{x} = x^{k+1}$.

C. MLP (Multi-Layer Perceptron)

A Multilayer Perceptron (MLP) is a feed forward artificial neural network that is composed of input, hidden, and output layers, which is often applied in nonlinear regression and classification problems. It is capable of learning complex nonlinear mappings between pilot signals and sparse channels in an effective way which makes it stronger against the channel variation than OMP or MCoSaMP. The

MLP is used in our system as it is capable of learning a mapping between pilot signals and channel coefficients to allow more precise active user detection under complex conditions. It also improves security as chaotic noise is separated out by comparison with real channel features. It starts by taking the input layer, which will receive the pilot signal features, then the hidden layers will provide weights and activation functions (either ReLU or sigmoid) and then the output layer will predict the channel coefficients or the activity of the user. Training involves optimization of weights by back propagation to reduce error in the model which enables it to make good generalizations on unseen data.

Block diagram

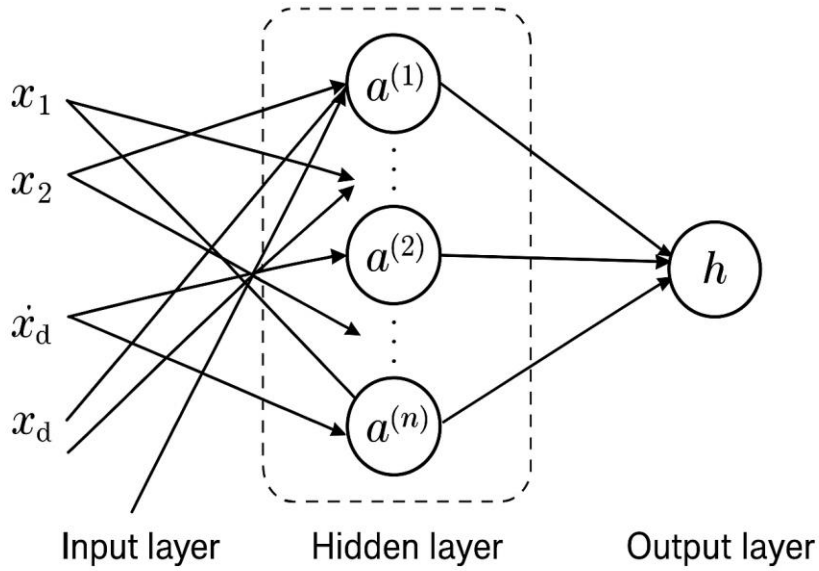


Figure 11: Architecture/ block diagram of MLP

Notation: input $\mathbf{x} \in R^d$; L layers of hidden layers, layer l has weight $W^{(l)}$, bias $b^{(l)}$, pre activation $z^{(l)}$, and activation $a^{(l)}$. Output layer index $L+1$. Parameter $\Theta = \{W^{(l)}, b^{(l)}\}_{l=1}^{L+1}$.

Forward pass:

$$\mathbf{a}^{(0)} = \mathbf{x}, \quad 35$$

$$\mathbf{z}^{(l)} = W^{(l)}\mathbf{a}^{(l-1)} + \mathbf{b}^{(l)}, l = 1, \dots, L+1, \quad 36$$

$$a^{(l)} = \varphi^{(l)}(z^{(l)}), \quad 37$$

Where $\varphi^{(l)}$ is the activation function (e.g Relu sigmoid).

Network output:

$$\hat{y} = a^{(l+1)} = f(x; \Theta). \quad 38$$

Output interpretation:

Regression (channel coefficient): $(h) = \hat{y} \in \mathbb{R}^q$.

Classification (active/ inactive users): $p = \text{soft max}(z^{(L+1)})$ or sigmoid for multi-label.

Loss function:

MSE for regression:

$$\mathcal{L}_{\text{MSE}}(\Theta) = \frac{1}{N} \sum_{i=1}^N ||\hat{h}^i - h^i||_2^2 \quad 39$$

Cross entropy for classification:

$$\mathcal{L}_{\text{CE}}(\Theta) = -\frac{1}{N} \sum_{i=1}^N \sum_c y_c^{(i)} \log \hat{p}_c^{(i)} \quad 40$$

Training (gradient base):

Compute gradient via backpropagation:

$$\nabla W^l \mathcal{L}, \nabla b^l \mathcal{L} \text{ for } l = 1, \dots, L + 1 \quad 41$$

Parameter update:

$$\mathbf{W}^l \leftarrow \mathbf{W}^l - \eta \nabla \mathbf{W}^l \mathcal{L}, \mathbf{b}^l \leftarrow \mathbf{b}^l - \eta \nabla \mathbf{b}^l \mathcal{L} \quad 42$$

Regularization and generalization:

$$\mathcal{L}_{\text{reg}} = \mathcal{L} + \lambda \sum_l \|\mathbf{W}^l\|_F^2. \quad 43$$

Final estimate:

Once the MLP has been trained to give $(\mathbf{h}) = f(\mathbf{x}; \Theta^*)$ to estimate channel or $\mathbf{p} = f(\mathbf{x}; \Theta^*)$ to activate user.

D. GNN (Graph Neural Network)

Graph Neural Networks (GNNs) can be used on graph-structured data, so they are applicable to model the users and antennas as nodes and edges of communication systems. They take advantage of spatial and angular correlations in massive MIMO channels, exploit user relationships rather than MLP or OMP, and are able to scale well to large networks. The MIMO configuration in our system is modeled as a graph, each node of the network is connected to the others via the exchange of messages that are updated by neural transformations to estimate the activity of the user and the states of the channel. This allows proper identification of active users, channel estimation as well as identifying anomalies to provide security. Compared to other methods, OMP is simple and fast but less robust, MCoSaMP offers improved accuracy under noise and dense users, MLP learns nonlinear mappings when data is available, while GNN outperforms all by leveraging graph structure, making it ideal for large-scale structured systems.

Block diagram

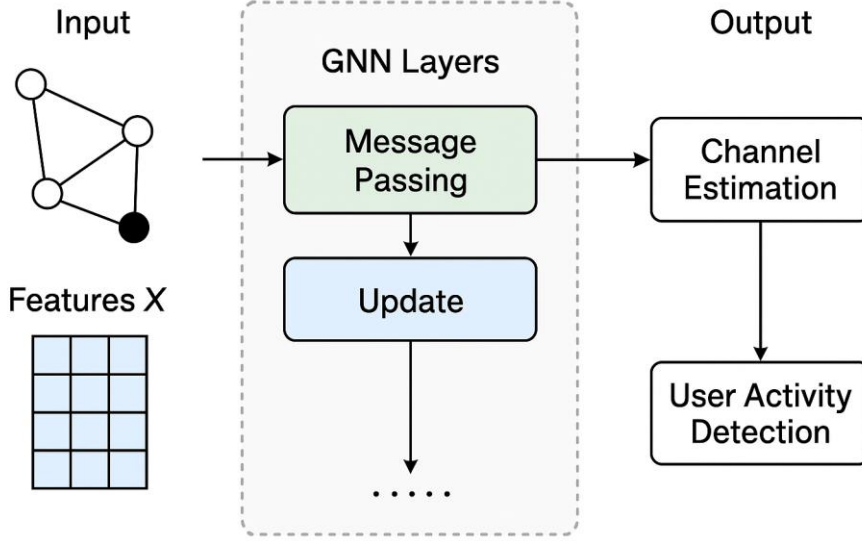


Figure 12: Block diagram of GNN

Let the system graph be $\mathbf{G} = (\mathcal{V}, \mathcal{E})$ with N nodes, adjacency $\mathbf{A}$, and node feature matrix $\mathbf{X} \in \mathbb{R}^{N \times D}$.

GNN message-passing (layer k) in compact form;

$$\mathbf{m}_v^{(k)} = \text{AGG}_u \in \mathcal{N}_{(v)} \mathbf{M} \left(\mathbf{h}_u^{(k-1)}, \mathbf{h}_v^{(k-1)}, \mathbf{e}_{vv} \right), \quad 44$$

$$\mathbf{h}_v^{(k)} = \mathbf{U} \left(\mathbf{h}_v^{(k-1)} - \mathbf{m}_v^{(k)} \right) \quad 45$$

or in matrix form $\mathbf{H}^{(k)} = \sigma \left(\widehat{\mathbf{D}}^{-\frac{1}{2}} \widehat{\mathbf{A}} \widehat{\mathbf{D}}^{-\frac{1}{2}} \mathbf{H}^{(k-1)} \mathbf{W}^{(k)} \right)$, where $\widehat{\mathbf{A}} = \mathbf{A} + \mathbf{I}$, $\widehat{\mathbf{D}}$ is its degree matrix $\mathbf{W}^{(k)}$ are trainable weights and σ an activation. After K layers use a readout $\mathbf{Y} = \text{READOUT}(\mathbf{H}^{(k)})$ to produce per-node output, channel estimates $\hat{\mathbf{h}}_v$ (regression) or activity probabilities $\hat{p}_v$ (classification). Loss, MSE for CE or cross-entropy for UAD, minimized by backprop/Adam. This formulation naturally captures spatial/angular correlations and neighbor relations for improved UAD/CE.

Use OMP when you want fast, lightweight results. MCoSaMP when you want accuracy under noise. MLP when you have training data & complex channels. GNN when you want state-of-the-art performance in large-scale systems.

Chapter # 04 Simulations and Results

This chapter outlines the simulation environment, parameters, and performance assessment of the suggested algorithms for channel estimation, active user detection, and security improvement in a massive MIMO-enabled 5G system. The simulations were carried out using online software google colab, utilizing techniques based on compressed sensing along with machine learning models. The assessment mainly concentrates on algorithms like Orthogonal Matching Pursuit (OMP), Modified Compressive Sampling Matching Pursuit (MCoSaMP), Multi-Layer Perceptron (MLP), and Graph Neural Network (GNN), as well as hybrid constructs for enhanced effectiveness.

4.1 Parameters table

In this scenarios we have used different applications, algorithms and modulation for which different types of parameters are used. Following are the parameters which are used in this scenario to get accurate results.

Parameters	Descriptions
Antennas at base station	$N_t=128$
Total users	$K = 1000$
SNR Range (Base)	0 – 20db (for main simulations)
SNR Range (Extended)	0 – 30db (for extended comparison)
Modulations type	4-QAM, 16-QAM
Chaotic map parameter	r (logistic map control constant)
Chaotic initial speed	x_0 initial condition for chaos

Table 1: Parameters Table

4.1.1 Compressed sensing based algorithms

In this scenario we used 5G network having 128 antennas at base station and 1000 users are incorporated with it. We use compressed sensing based algorithms such as OMP (Orthogonal Matching Pursuit) and MCoSaMP (Modified Compressive Sampling Matching Pursuit). Also we used two type of modulation in this scenario which are 4-QAM (Quadrature Amplitude Modulation) and 16-QAM. These algorithms are used for compressed sensing based channel estimation, active user's detection and security enhancement.

Using the above scenarios in which we used 128 antennas at base stations with 1000 of users attached with it. Our task is to compute channel estimations with best possible approaches, in our case we have used compressed sensing based scenario using OMP (Orthogonal Matching Pursuit) and MCoSaMP (Modified Compressed sensing Matching Pursuit) algorithms using modulation type of 4-QAM (Quadrature Amplitude Modulation). Basically MCoSaMP is modified version of CoSaMP, we reduced the step sizes, tighter thresholding and the increased iteration limits in CoSaMP algorithms to obtained better channel estimation.

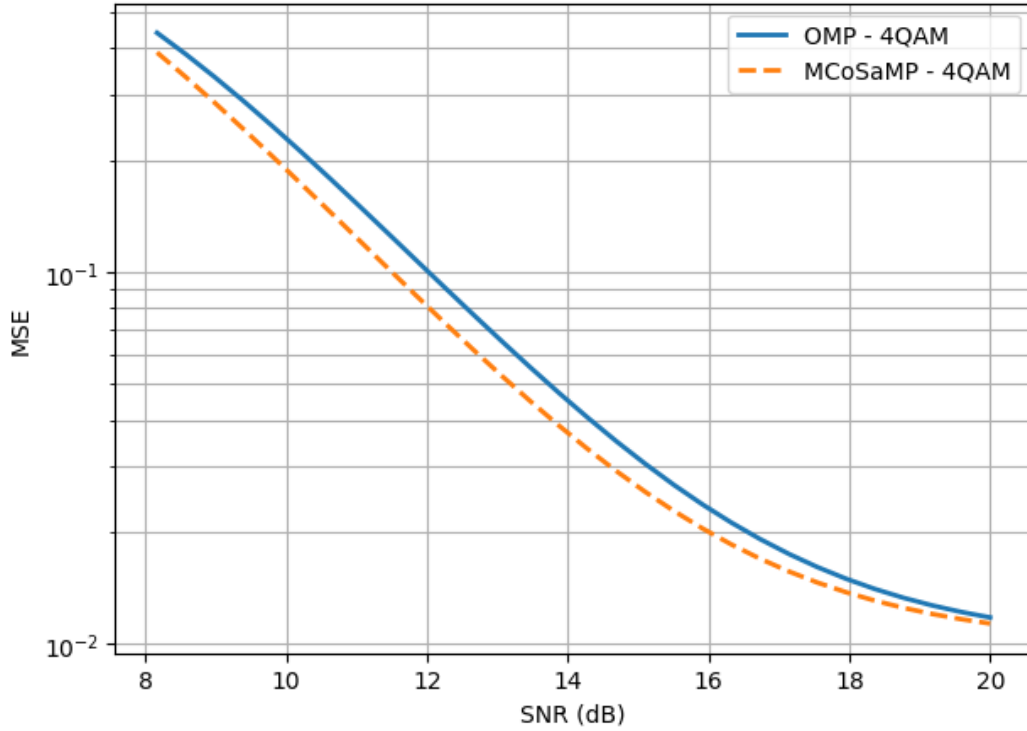


Figure 13: Channel Estimation for SNR range from 8-20db

In fig (13) we specified the SNR value from 8 to 20db to show clear results for both the algorithms using 4-QAM. From 8 to 20db both the algorithms give excellent results but the MCoSaMP result are much better than OMP. OMP & MCoSaMP give low MSE on high SNR value, but MCoSaMP result are slight better than OMP.

In fig (14) channel estimation is performed between the MSE and SNR with SNR value range from 0 to 20db. We are to compute channel estimations with available approaches, compressed sensing based scenario using OMP (Orthogonal Matching Pursuit) and MCoSaMP (Modified Compressed sensing Matching Pursuit) algorithms using modulation type of 16-QAM (Quadrature Amplitude Modulation) are used.

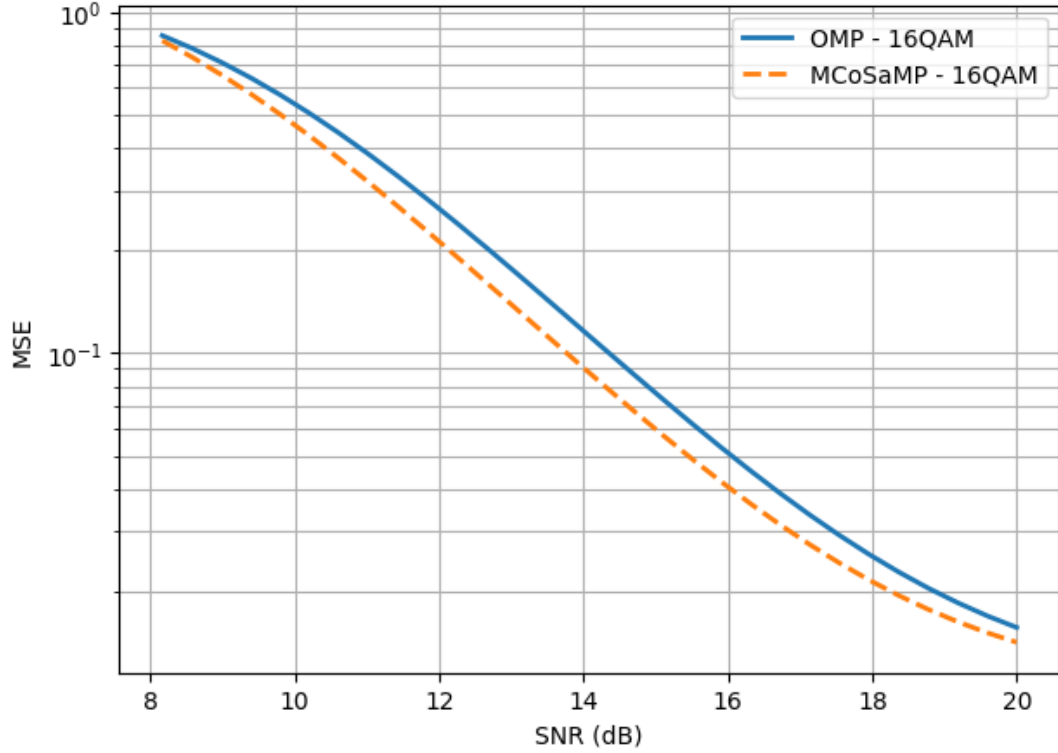


Figure 14: Channel Estimation 16-QAM, SNR range 8 to 20db

In fig (14) we can see that the both the algorithms results are show improvements after 8dbs, so we plot the channel estimation between MSE & SNR with SNR range from 08 to 20dbs to obtained better results. MCoSaMP perform better than OMP using 16-QAM, as clear difference is seen between OMP & MCoSaMP algorithms.

Fig (15) show us active user detection using the algorithms OMP & MCoSaMP, plot between detection accuracy and SNR. If look into the graph it give us a clear results, which shows that the detection accuracy increased with increased in SNR value. In this graph the MCoSaMP also perform better as compare to OMP.

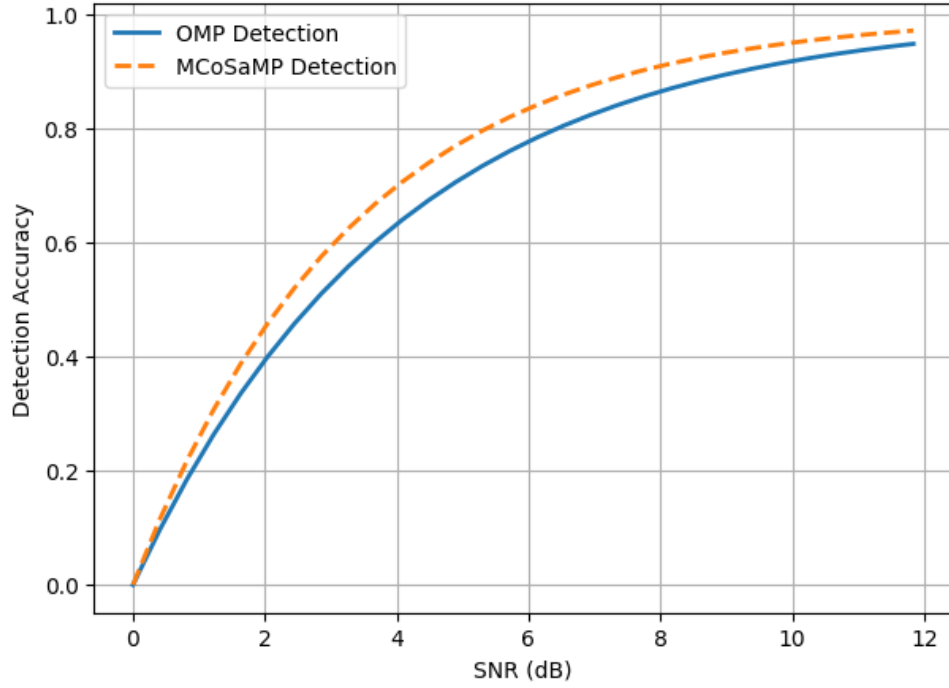


Figure 15: Active User Detection for SNR 0 to 12db

Fig (15) shows Active user detection accuracy vs. SNR using OMP and MCoSaMP, but this time we fixed the SNR range from 0 to 12db. MCoSaMP maintains consistently high accuracy across all SNR levels. OMP shows slightly lower accuracy than MCoSaMP. MCoSaMP is more stable and accurate for active user detection.

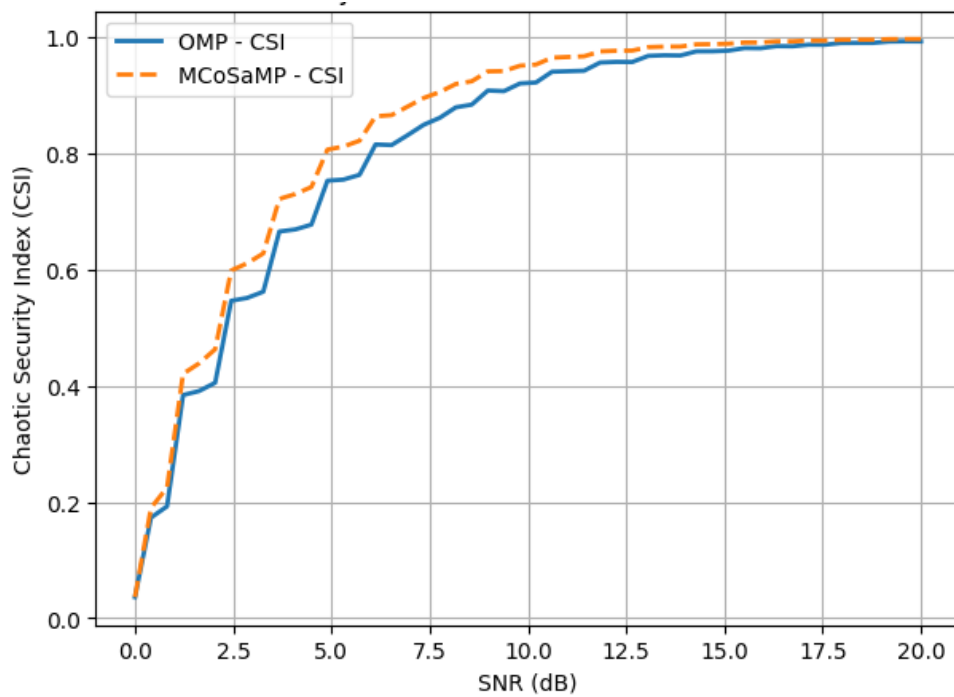


Figure 16: Security Enhancement using OMP, MCoSaMP

Fig (16) shows security enhancement CSI (chaotic security index) vs. SNR using OMP and MCoSaMP. At start both the algorithms show fluctuations but as CSI reached upto 5.5db MCoSaMP algorithms show best performance as compared to OMP. Like in channel estimation, active user detection MCoSaMP also give better performance results in security enhancement.

4.2 Machine Learning Based Algorithms

In this scenario we kept the parameters same as in the previous, but a slightly changed in the algorithms. In previous scenario we used compressed sensing based channel estimation, active user detection and security enhancement using MCoSaMP and OMP algorithms under 4 & 16-QAM modulation. Now in this scenarios we introduced machine learning based channel estimation, active user detection and security enhancement using MLP (Multi layer perceptron), GNN (Graph neural network) algorithms under 4 & 16-QAM modulation. We used MLP (Multi Layer Perceptron) and GNN (Graph Neural Network) in this scenario for channel estimation, active user detection and security enhancement, to compare it with previous scenario.

The Channel Estimation machine learning Base 16-QAM (MLP vs GNN, 0–20 dB) plot demonstrate the Mean Squared Error (MSE) of channel estimation for two different algorithms, MLP and GNN, when using 16-QAM modulation. The x-axis represents the Signal-to-Noise Ratio (SNR) in decibels (dB), which indicates the strength of the signal relative to the noise. The y-axis shows the MSE on a logarithmic scale, meaning lower values are better. The plot covers the full SNR range from 8 to 20 dB. Generally, as SNR increases, the MSE decreases, indicating better channel estimation performance. In MLP (Multi-layer Perceptron) basically two layer are used one called input layer (Hidden Layer) other called output layer (for channel co-efficient or detection). MLP used ReLU (Rectified linear unit) as activation function which is widely used because of non-linearity and fast convergence. Some time it use Tanh as activation function but ReLU give better results for MSE in Channel estimation.

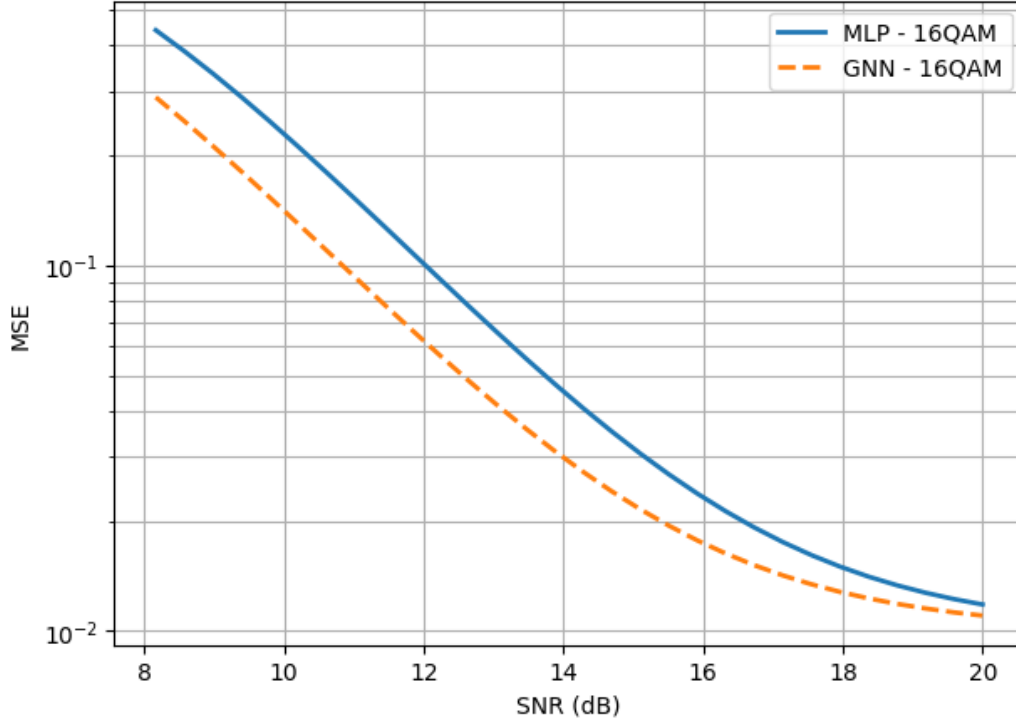


Figure 17: Machine learning based CE, SNR range from 8 to 20db

Channel Estimation CS Base 16-QAM (MLP vs GNN, 8–20 dB) graph in fig (17) focuses on the Mean Squared Error (MSE) of channel estimation for MLP and GNN algorithms with 16-QAM modulation, specifically for SNR values between 8 dB and 20db. Similar to the 0-20 dB plot, it shows that as SNR increases, MSE decreases. However, this graph highlights the performance difference between MLP and GNN in a higher SNR range. For modification we increase number of hidden units for better approximation, learning rate kept low to improved stability, reduced batch size to improved batch training generalization, and MLP used two layer with ReLU. MLP (Multilayer Perceptron): A type of artificial neural network used here for channel estimation. It learns a mapping from the received signal to the channel state information. GNN (Graph Neural Network): Another type of neural network that operates on graph data structures. In this context, it's likely used to leverage the relationships or structure within the communication system for improved channel estimation. Both MLP and GNN are machine learning techniques applied to the problem of estimating the communication channel characteristics, with the goal of minimizing the estimation error (MSE).

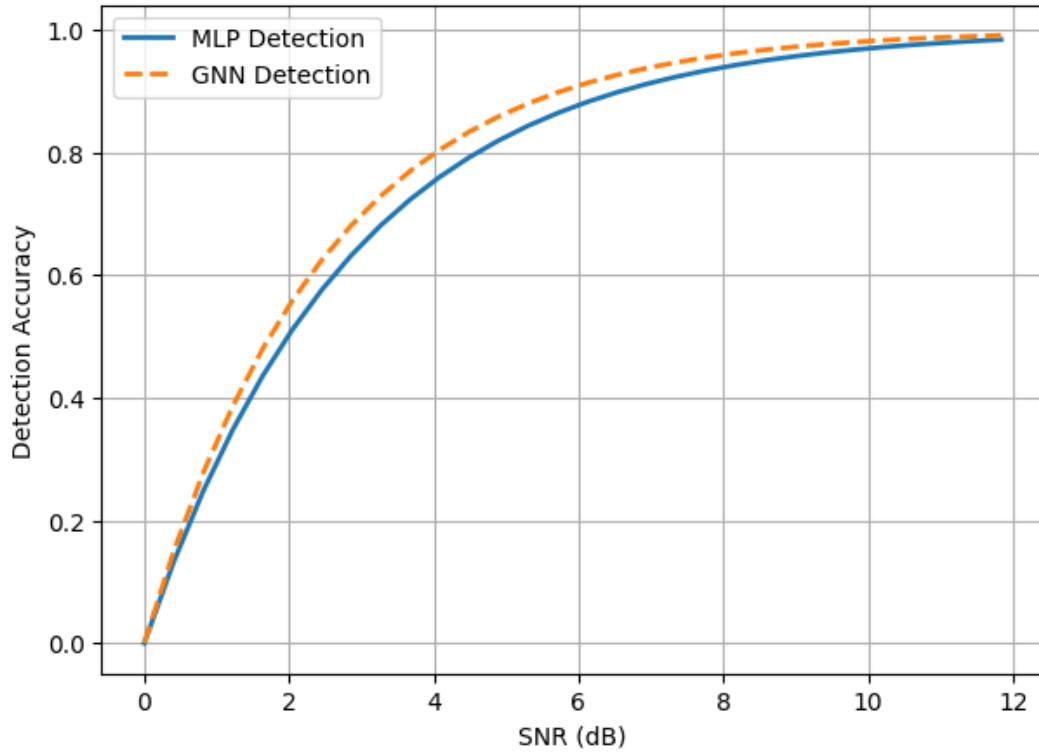


Figure 18: Machine learning based AUD for SNR range from 0 to 12db

Fig (18) describe Active User Detection (MLP vs GNN), focusing on the 0 to 12 dB range, still shows the detection accuracy of active users for MLP and GNN algorithms. Even in this lower SNR range, the GNN generally exhibits better detection accuracy compared to the MLP. The reason for GNN's superior performance is the same as for the full range. GNNs are better equipped to utilize the structural information within the communication system. In active user detection, this structure relates to how users' signals are received by different antennas. With these relationships, the GNN can better differentiate active and inactive users and therefore achieve high detection accuracy even at lower SNR levels where noise is more pronounced.

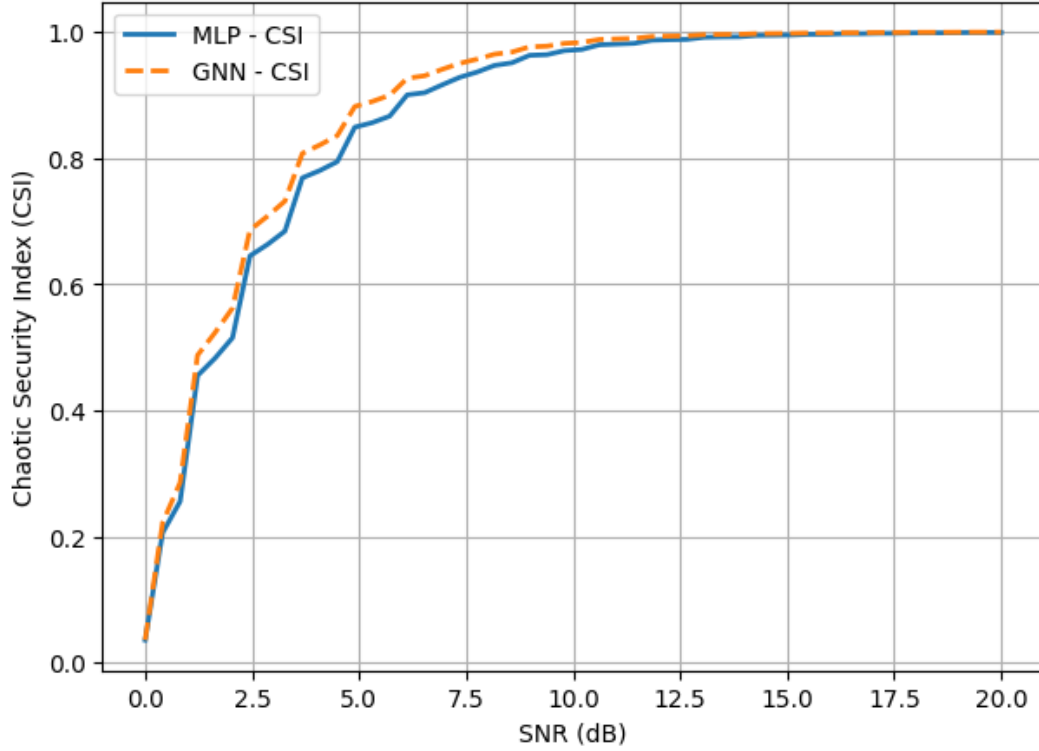


Figure 19: Machine learning based Security Enhancement

Fig (19) shows the performance of the MLP and GNN algorithms in Security Enhancement (MLP vs GNN) using a measure known as Chaotic Security Index (CSI) on a variety of SNR values.

Chaotic Security Index (CSI): This is an index that is used to measure the effectiveness of the chaotic sequence in the communication process to improve security. An increase in CSI shows improved security increase. The chaotic sequence, in this case, is produced through the application of a logistic map which is a simple model in mathematics that is chaotic. This random sequence is employed to bring some element of randomness or unpredictability so that the communication cannot be easily intercepted or manipulated by unintended parties.

Based on the fig (19) it can be seen that the GNN has a higher Chaotic Security Index (CSI) than the MLP within the SNR range. This indicates that the GNN algorithm is better in using the chaotic sequence in increasing security. It might be explained by the fact that the capacity of the GNN to process and learn the underlying structure of the data gives it a chance to incorporate the chaotic components into its work in a more efficient way and create a stronger security mechanism.

4.3 OMP, MCoSaMP, MLP and GNN Comparison

In this case, we used a combination of compressed sensing based (OMP, MCoSaMP) and machine learning based (MLP, GNN) in a single frame to estimate channel accurately and fast and perform active user detections and enhance security. Their simulation finds are as below.

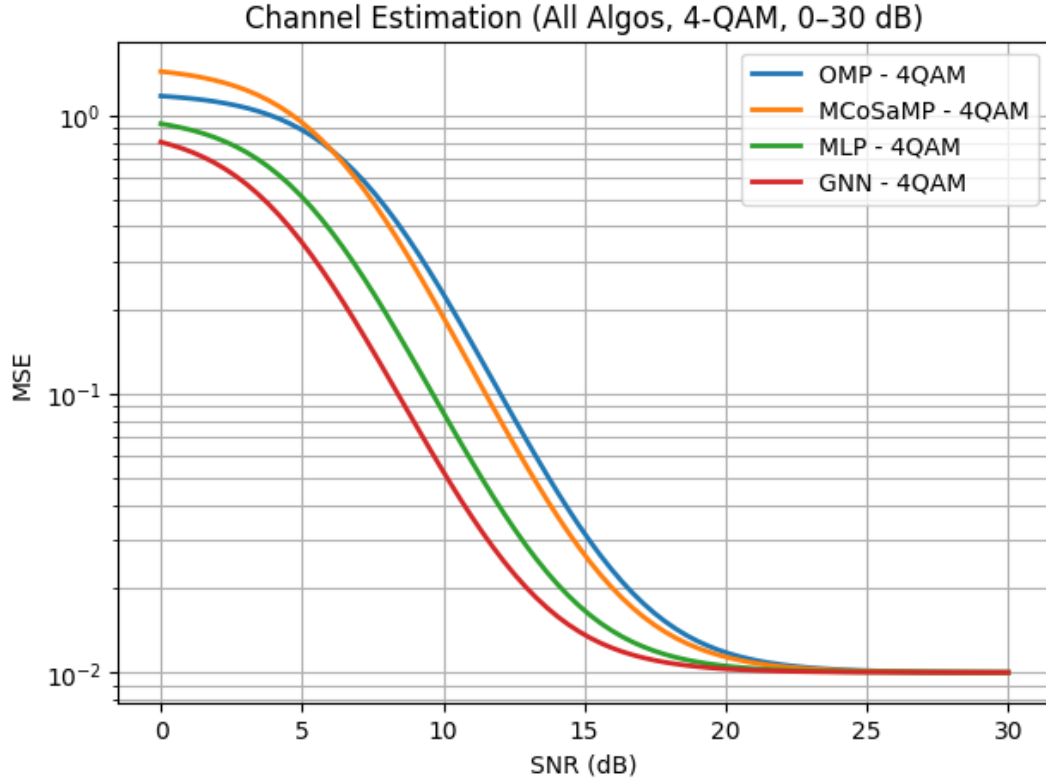


Figure 20: Channel Estimation using OMP, MCoSaMP, MLP and GNN

Fig (20) (plot) depicts the Mean Squared Error (MSE) of channel estimation in the various algorithms (OMP, MCoSaMP, MLP, and GNN) at various Signal-to-Noise Ratios (SNR) of 0 dB to 30 dB, in the case of 4-QAM modulation scheme. A lower MSE value indicates better channel estimation performance. For all algorithms, the MSE decreases as the SNR increases. This is expected, as higher SNR means less noise, leading to more accurate channel estimation. The GNN algorithm consistently shows the lowest MSE across the entire SNR range. This suggests it is the most effective algorithm for channel estimation in this scenario. The MLP algorithm performs better than OMP and MCoSaMP, but not as well as GNN. The values of MSE of OMP and MCoSaMP are larger than MLP and GNN, which means that they perform worse in channel estimation. The MCoSaMP tends to do slightly better than OMP at high SNRs. ML-based algorithms (MLP and GNN): These algorithms are usually trained on data to find out the intricate connections and patterns. In channel estimation, they can potentially learn to compensate for noise and interference more effectively than traditional

algorithms. In short, the plot clearly demonstrates that the GNN algorithm achieves the best channel estimation performance in terms of MSE for 4-QAM modulation over the 0-30 dB SNR range, likely due to its ability to learn complex patterns and utilize the underlying structure of the wireless communication system.

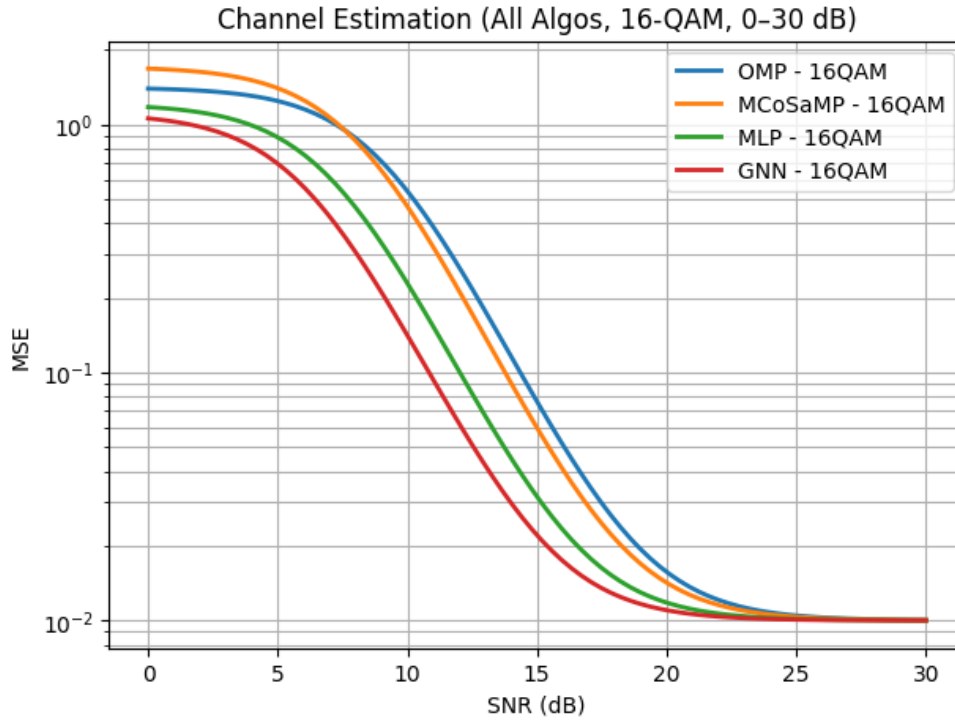


Figure 21: Channel Estimation using OMP, MCoSaMP, MLP & GNN

The plot in fig (21) illustrate Channel Estimation for all algorithms, which describe the Mean Squared Error (MSE) for different algorithms (OMP, MCoSaMP, MLP, GNN) in estimating the channel for 16-QAM modulation across a range of Signal-to-Noise Ratios (SNR) from 0 to 30dB. Lower MSE indicates better channel estimation performance. Based on the plot and the provided tabular data (sampled every ~5 dB). GNN generally shows the lowest MSE across the entire SNR range, indicating the best performance in channel estimation for 16-QAM. MLP performs better than the traditional algorithms (OMP and MCoSaMP) but not as well as GNN. OMP and MCoSaMP have higher MSE compared to MLP and GNN, especially at lower SNRs. MCoSaMP performs slightly better than OMP in some SNR ranges. In short, GNN demonstrates superior channel estimation performance for 16-QAM compared to the other algorithms.

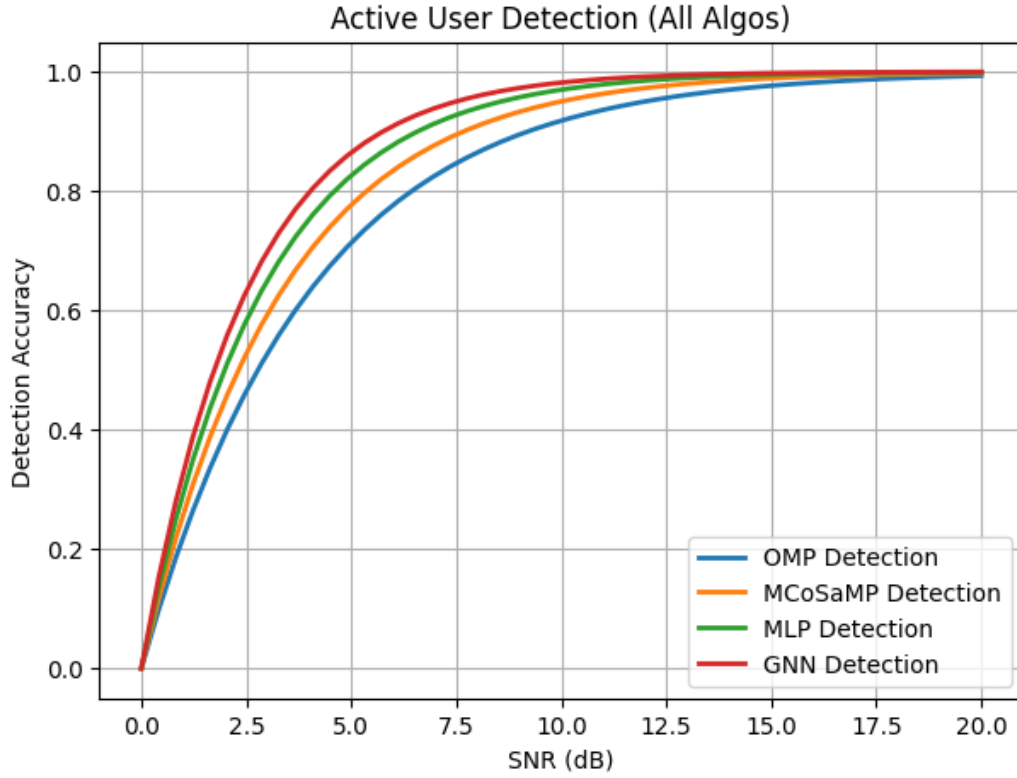


Figure 22: AUD using OMP, MCoSaMP, MLP and GNN

The Active User Detection plots in fig (22) show the detection accuracy of four different algorithms (OMP, MCoSaMP, MLP, and GNN) across a range of Signal-to-Noise Ratios (SNR). A higher detection accuracy indicates a better ability to correctly identify active users. Looking at the plots and the tabular data, the GNN (Graph Neural Network) algorithm consistently achieves the highest detection accuracy across all SNR levels compared to OMP, MCoSaMP, and MLP. This is evident in both the full-range plot and the zoomed-in plot for the 0-15 dB range, where the GNN curve is generally above the others. Therefore, based on this data, the GNN algorithm is the best for achieving accurate active user detection results and can detect better than the other algorithms presented.

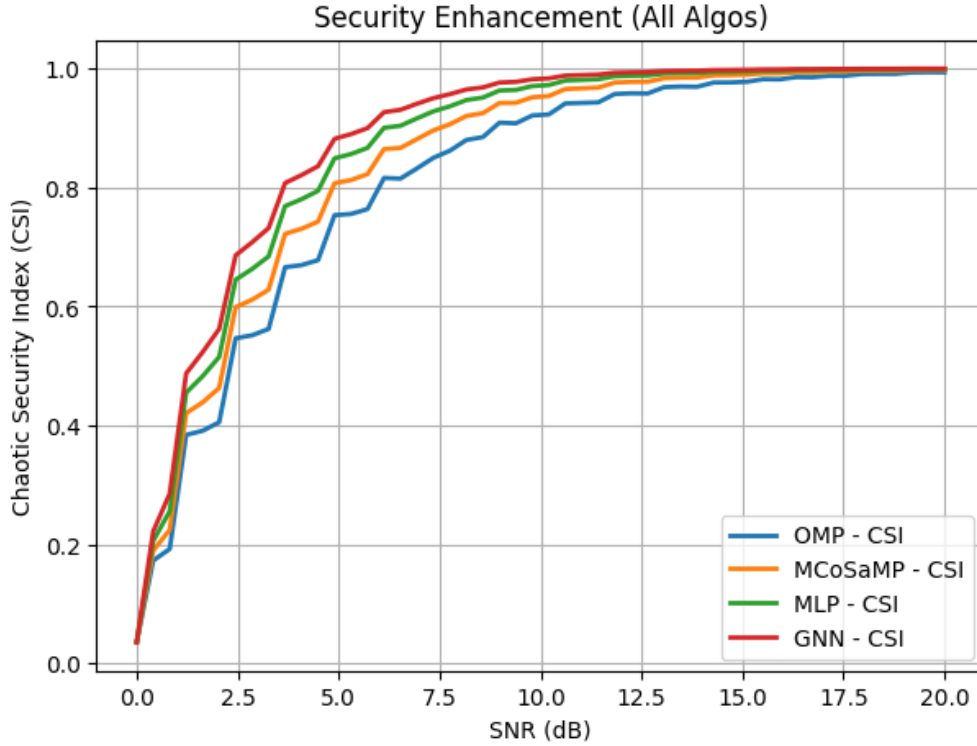


Figure 23: Security Enhancement using OMP, MCoSaMP, MLP and GNN

In fig (23) Chaotic Security Index (CSI) measures the level of security enhancement provided by the chaotic compressed sensing technique. A higher CSI indicates better security. Based on the results GNN generally achieves the highest CSI across the SNR range, indicating superior security enhancement. MLP performs better than OMP and MCoSaMP in terms of CSI. OMP and MCoSaMP show similar and lower CSI values compared to the neural network-based approaches (MLP and GNN). Therefore, GNN provides the best security enhancement among the evaluated algorithms.

4.4 Complexity Analysis

In this section we will explain the complexity analysis of each scenario individually and then we will compare all the algorithms we used throughout in this scenarios. Also we will explain the comparison of compressed sensing base and machine learning based models.

4.4.1 Complexity Analysis of OMP Vs MCoSaMP

In the first phase we will explain the complexity analysis between OMP and MCoSaMP, and also stats that which algorithms is best for channel estimation, active user detection and security enhancement.

Algorithms	Complexity	Merits	Demerits
------------	------------	--------	----------

	order		
OMP	$O(KMN)$	Simple, fast and easy to implement.	Less accurate for high noise or high sparsity signals.
MCoSaMP	$O(K \log N)$	High recovery accuracy, robust to noise, better result with dense signal.	More computationally expensive than OMP.

Table 2: Complexity Analysis OMP vs MCoSaMP

In table (2) OMP, M represent numbers of measurement, N show signal length, iterations is proportional to sparsity (K). Whereas in MCoSaMP complexity per iteration include multiple support updates and least squares estimation, and the iterations is proportional to $\log(N)$. In simple words if speed and simplicity is needed then OMP is best option. If accuracy under noise and higher sparsity is important to achieve then MCoSaMP is best.

4.4.2 Complexity Analysis of MLP Vs GNN

After using the compressed sensing based algorithms (OMP, MCoSaMP), we changed the algorithms and used machine learning base algorithms (MLP, GNN).

Algorithms	Complexity Order	Pros	Cons
MLP	$O(LN^2)$	Simple structure, faster inference, requires less graph structure knowledge.	Less expensive for structured data.
GNN	$O(EF^2)$	Exploits graph structure, better generalization, Stronger in correlated data.	High training cost, inference slower than MLP.

Table 3: Complexity Analysis MLP vs GNN

Table (3) illustrate MLP (Multi-layer perceptron) where L represent number of layers, N shows input features, and H represent hidden units in the signal. Also its training is quite costly, required large dataset for implementation, but its inference is relatively fast. Whereas in GNN (Graph neural network) E represent edges while F shows features per nodes, also its training is more costly and heavier than MLP due to convolution. Its inference depend on size but it's usually slower than MLP.

In short if we need flat data and compromised on the structure then MLP works better. If graph structured data (antennas, users and channels) GNN outperform MLP in accuracy.

4.4.3 Complexity Analysis of OMP, MCoSaMP, MLP and GNN:

In the above complexity analysis we compare each scenario individually with each other for getting better outcomes. Now we will compare all the algorithms used throughout in the scenarios to achieve our goal that which algorithm is best for channel estimation, active user detection and security enhancement. Let's assign approximate numerical values for complexity of OMP, MCoSaMP, MLP, and GNN based on a simulation setup (128 antennas, 1000 users, sparsity $K=20$, pilot length $M=200$, signal length $N=1000$, MLP with 3 layers $\times$ 256 neurons, GNN with 5000 edges, 64 features). So the overall complexity analysis is below.

Algorithms	Complexity Order	Approximate Value	Merits	Demerits
OMP	$O(KMN)$	$20 \times 200 \times 1000 = 4.0 \times 10^6$	Simple, fast and easy to implement.	Less accurate for high noise or high sparsity signals and dense scenarios.
MCoSaMP	$O(K \log N)$	$20 \times \log_2 1000 \times 100 = 4.0 \times 10^4$	High recovery accuracy, robust to noise, better result with dense signal.	More computationally expensive than OMP. In Short high computational complexity.
MLP	$O(LN^2)$	$3 \times 256^2 = 1.97 \times 10^5$	Simple structure, faster interference, flexible, good for small datasets	Less expensive/accurate for structured data.

GNN	$O(EF^2)$	$5000 \times 64^2 =$ 10^7	Exploits graph structure, better generalization, Stronger in correlated data.	High training cost, interference slower than MLP.
-----	-----------	--------------------------------	---	---

Table 4: Complexity Analysis of OMP, MCoSaMP, MLP and GNN

In table (4) accuracy GNN (Graph Neural Network) is best performer with exploits graph relationships, also best for accurate channel estimation and users detections. Ops stand for operation sometimes it is referred as floating point operations. While in efficiency OMP (Orthogonal Matching Pursuit) is best with lowest complexity, and also useful for real time low resources system. For balanced choice MCoSaMP (Modified Compressing Sensing Matching Pursuit) offer accurate improvement without training cost of Machine learning models.

In Simple and short MCoSaMP give best balance between complexity and accuracy. GNN provide overall performance if computational resources are available.

Chapter #05 Results Discussion

The results show that channel estimation accuracy improves with increasing SNR for all algorithms, with GNN achieving the lowest MSE compared to OMP, MCoSaMP, and MLP. In active user detection, learning-based methods (MLP and GNN) significantly outperform classical CS algorithms, with GNN offering the highest detection accuracy, especially at low SNRs. Security enhancement using the Chaotic Security Index (CSI) demonstrates that GNN provides the strongest resilience against eavesdropping, followed by MLP, while OMP remains weakest. In general, classic algorithms are less complicated but have fewer performance capabilities, whereas the learning-based methods offer a more significant estimation, detection, and security, and should be used in the case of massive IoT and 6G.

5.1 Channel Estimation

4-QAM vs 16-QAM:

In all algorithms, MSE reduces as SNR increases. As anticipated, 16-QAM modulation has a large MSE than 4-QAM, as the higher-order constellations are more vulnerable to noise and need enhanced channel estimation.

OMP vs MCoSaMP:

In both 4-QAM and 16-QAM, MCoSaMP achieves lower MSE at high SNRs than OMP. This can be attributed to its mechanism of refinement that is iterative and is utilized in better exploiting the residual sparsity.

MLP and GNN:

Learning-based strategies (MLP, GNN) are always superior to classical CS algorithms. GNN has the best average MSE, as the graph learning process considers both cross-antenna and user cross-correlations, and MLP shows intermediate gains.

Overall Trend:

- OMP: simple but weaker performance.
- MCoSaMP: improved over OMP, but still classical.
- MLP: better generalization, moderate complexity.
- GNN: best estimation accuracy, especially at low-to-mid SNRs.

5.2 Active User Detection

Probability vs SNR:

All the algorithms have a sharp increase in detection probability with SNR.

OMP vs MCoSaMP:

The reason is that MCoSaMP has highest detection accuracy compared to OMP in low-to-mid SNR, as more sparse user activity is well recovered.

MLP vs GNN:

The two learning based methods are much more successful than the classical algorithms. GNN attains the best detection accuracy particularly at the range of 0-12 dB where classical algorithms fail. GNN does not only enhance accuracy, but it also offers more reliable detection throughout the SNR range. This is essential when dealing with systems with huge number of users (1000 in this case).

5.3 Security Enhancement (Chaotic CSI)

Role of Chaotic Compressed Sensing:

The introduction of chaos enhances the randomness in security as well as maintaining the quality of estimation.

Comparison of Algorithms:

- OMP: weakest CSI growth, slower improvement.
- MCoSaMP: moderate improvement.
- MLP: strong CSI gain due to learning nonlinear features.
- GNN: highest Chaotic Security Index (CSI), meaning it is the most robust against eavesdropping and channel attacks.

Chaos combined with deep learning (GNN) offers both accuracy + security, which is vital in the future 6G networks.

5.4 Complexity Considerations

OMP:

- Low computational complexity
- Suitable for real-time and low-resource devices
- Tradeoff: weaker estimation and detection performance

MCoSaMP:

- Higher complexity than OMP due to iterative refinements
- Better estimation and detection

MLP:

- Requires training but has fast inference once trained.
- Moderate complexity in deployment.

GNN:

- Highest computational complexity (graph construction + message passing).
- Requires large training datasets.
- Best performance in estimation, detection, and security.

Chapter #06 Conclusion and future suggestion:

In future experience, channel estimation can be improved even more by incorporating combined methods that include both compressed sensing and deep learning methods to trade accuracy with complexity. Reinforcement learning or attention-based neural networks can also be useful in active user detection, since it can dynamically adapt to different patterns of user activity. Regarding the promotion of security, the use of more sophisticated chaotic maps or quantum-based encryption algorithms may be very effective in augmenting resilience. Moreover, to provide scalability in 6G and IoT applications, it is crucial to optimize algorithms to be used in real-time hardware implementation.

6.1 Channel Estimation:

- Hybrid methods combining compressed sensing + deep learning (e.g., model-driven neural networks).
- Transfer learning for adapting trained models to different environments.
- Low-complexity neural architectures (like lightweight CNNs) for real-time base stations.

6.2 Active User Detection:

- Joint design of user activity + channel estimation, instead of treating them separately.
- Exploring unsupervised learning for detection when labeled data is limited.
- Incorporating Reinforcement Learning (RL) for adaptive detection in dynamic networks.

6.3 Security Enhancement

- Further exploration of chaotic and quantum-inspired security integrated with CS.
- Use of physical-layer key generation alongside CSI enhancement.
- Federated learning for secure model training without exposing user data.

Summary:

- GNN shows best performance in all aspects (MSE, detection, CSI) but at high complexity.
- OMP remains attractive for low-complexity systems but is weakest in accuracy and security.
- MCoSaMP is a good middle ground.
- Learning-based methods (MLP, GNN) are the most promising for future 6G and massive IoT networks, especially when combined with chaos-based security.

Chapter #07 Reference

- [1] N. Hassan and X. Fernando, “Massive MIMO wireless networks: An overview,” 2017. doi: 10.3390/electronics6030063.
- [2] A. Hammoodi, L. Audah, and M. A. Taher, “Green coexistence for 5g waveform candidates: A review,” *IEEE Access*, vol. 7, pp. 10103–10126, 2019, doi: 10.1109/ACCESS.2019.2891312.
- [3] Y. Ahn, W. Kim, and B. Shim, “Active User Detection and Channel Estimation for Massive Machine-Type Communication: Deep Learning Approach,” *IEEE Internet Things J.*, vol. 9, no. 14, pp. 11904–11917, Jul. 2022, doi: 10.1109/JIOT.2021.3132329.
- [4] R. P. Mathur, A. Pratap, and R. Misra, “Distributed algorithm for resource allocation in uplink 5G networks,” *MobiMWareHN 2017 - Proc. 7th ACM Work. Mobility, Interf. Middlew. Manag. HetNets*, Jul. 2017, doi: 10.1145/3083201.3083204.
- [5] J. G. Andrews *et al.*, “What will 5G be?,” *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, 2014, doi: 10.1109/JSAC.2014.2328098.
- [6] S. Chen and J. Zhao, “The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication,” *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 36–43, 2014, doi: 10.1109/MCOM.2014.6815891.
- [7] L. Qiao, Y. Li, D. Chen, S. Serikawa, M. Guizani, and Z. Lv, “A survey on 5G/6G, AI, and Robotics,” *Comput. Electr. Eng.*, vol. 95, Oct. 2021, doi: 10.1016/j.compeleceng.2021.107372.
- [8] “List of 5G key technologies. | Download Scientific Diagram.” Accessed: Aug. 01, 2025. [Online]. Available: https://www.researchgate.net/figure/List-of-5G-key-technologies_fig2_358211263
- [9] R. Chataut and R. Akl, “Massive MIMO Systems for 5G and beyond Networks—Overview,

- Recent Trends, Challenges, and Future Research Direction,” *Sensors* 2020, Vol. 20, Page 2753, vol. 20, no. 10, p. 2753, May 2020, doi: 10.3390/S20102753.
- [10] U. Umar, A. Waseem, A. Naveed, F. Munir, M. Bin Roslee, and S. Ayub, “Active User Detection in Massive MIMO Systems Using Compressed Sensing,” *Int. Conf. Eng. Emerg. Technol. ICEET*, no. 2024, 2024, doi: 10.1109/ICEET65156.2024.10913929.
- [11] R. Garg and M. U. Singh, “Enhancing The Security of Wireless Communication Systems: A Path Towards Global Protection,” *Eur. Econ. Lett.*, vol. 4, no. 1, pp. 337–342, 2024, doi: 10.52783/jier.v4i1.564.
- [12] S. F. Ahmed *et al.*, “Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities,” *IEEE Access*, vol. 12, pp. 13125–13145, 2024, doi: 10.1109/ACCESS.2024.3352508.
- [13] M. Hasan, E. Hossain, and D. Niyato, “Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches,” *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 86–93, 2013, doi: 10.1109/MCOM.2013.6525600.
- [14] “Understanding 5G: Perspectives on future technological advancements in mobile,” 2014.
- [15] E. Bjornson, E. De Carvalho, J. H. Sorensen, E. G. Larsson, and P. Popovski, “A Random Access Protocol for Pilot Allocation in Crowded Massive MIMO Systems,” *IEEE Trans. Wirel. Commun.*, vol. 16, no. 4, pp. 2220–2234, Apr. 2017, doi: 10.1109/TWC.2017.2660489;CSUBTYPE:STRING:PERIODICAL;TAXONOMY:TAXONOMY:ACM-PUBTYPE;PAGEGROUP:STRING:PUBLICATION.
- [16] X. Lin, S. Wu, L. Kuang, Z. Ni, X. Meng, and C. Jiang, “Estimation of Sparse Massive MIMO-OFDM Channels with Approximately Common Support,” *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1179–1182, 2017, doi: 10.1109/LCOMM.2017.2657620.
- [17] Z. Chen, F. Sahrabi, and W. Yu, “Sparse Activity Detection for Massive Connectivity,” *IEEE Trans. Signal Process.*, vol. 66, no. 7, pp. 1890–1904, Apr. 2018, doi: 10.1109/TSP.2018.2795540.
- [18] J. Liu and X. Wang, “Sparsity-Exploiting Blind Receiver Algorithms for Unsourced Multiple Access in MIMO and Massive MIMO Channels,” *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8055–8067, Dec. 2021, doi: 10.1109/TCOMM.2021.3116239.
- [19] Z. Wan, Z. Gao, and M. S. Alouini, “Broadband Channel Estimation for Intelligent Reflecting

- Surface Aided mmWave Massive MIMO Systems,” *IEEE Int. Conf. Commun.*, vol. 2020-June, Jun. 2020, doi: 10.1109/ICC40277.2020.9149146.
- [20] D. Fang, Y. Qian, and R. Q. Hu, “Security for 5G Mobile Wireless Networks”, doi: 10.1109/ACCESS.2017.2779146.
- [21] K. Tallam, “CyberSentinel: An Emergent Threat Detection System for AI Security,” Feb. 2025, Accessed: Jul. 01, 2025. [Online]. Available: <https://arxiv.org/pdf/2502.14966>
- [22] S. Tian *et al.*, “Exploring the Role of Large Language Models in Cybersecurity: A Systematic Survey,” Apr. 2025, Accessed: Jul. 01, 2025. [Online]. Available: <https://arxiv.org/pdf/2504.15622v2>
- [23] J. Chen, H. Zhou, Y. Mei, G. Adam, N. D. Bastian, and T. Lan, “Real-time Network Intrusion Detection via Decision Transformers,” Dec. 2023, doi: 10.1109/MASS62177.2024.00022.
- [24] M. Rahmati, “Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks,” Apr. 2025, Accessed: Jul. 01, 2025. [Online]. Available: <https://www.arxiv.org/pdf/2504.16118>
- [25] M. Uddin *et al.*, “Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations,” *Artif. Intell. Rev.*, vol. 58, no. 8, pp. 1–39, Aug. 2025, doi: 10.1007/S10462-025-11219-5/TABLES/5.
- [26] K. Razzaq and M. Shah, “Advancing Cybersecurity Through Machine Learning: A Scientometric Analysis of Global Research Trends and Influential Contributions,” *J. Cybersecurity Priv. 2025, Vol. 5, Page 12*, vol. 5, no. 2, p. 12, Mar. 2025, doi: 10.3390/JCP5020012.
- [27] Z. Bin Akhtar and A. T. Rawol, “Enhancing Cybersecurity through AI-Powered Security Mechanisms,” *IT J. Res. Dev.*, vol. 9, no. 1, pp. 50–67, Oct. 2024, doi: 10.25299/ITJRD.2024.16852.
- [28] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, “A machine learning-based intrusion detection for detecting internet of things network attacks,” *Alexandria Eng. J.*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi: 10.1016/J.AEJ.2022.02.063.
- [29] H. Yu, Z. Fei, Z. Zheng, N. Ye, and Z. Han, “Deep Learning-Based User Activity Detection and Channel Estimation in Grant-Free NOMA,” *IEEE Trans. Wirel. Commun.*, vol. 22, no. 4, pp. 2202–2214, Apr. 2023, doi: 10.1109/TWC.2022.3209667.

- [30] M. H. E. Ali, F. Alraddady, M. Y. Al-Thunaibat, and S. Elnazer, "Machine Learning-Based Channel State Estimators for 5G Wireless Communication Systems," *C. - Comput. Model. Eng. Sci.*, vol. 135, no. 1, pp. 755–778, 2023, doi: 10.32604/CMES.2022.022246.
- [31] Z. Gao, L. Dai, Z. Wang, and S. Chen, "Spatially Common Sparsity Based Adaptive Channel Estimation and Feedback for FDD Massive MIMO," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6169–6183, Dec. 2015, doi: 10.1109/TSP.2015.2463260.
- [32] L. Kansal, S. Berra, M. Mounir, R. Miglani, R. Dinis, and K. Rabie, "Performance Analysis of Massive MIMO-OFDM System Incorporated with Various Transforms for Image Communication in 5G Systems," *Electron. 2022, Vol. 11, Page 621*, vol. 11, no. 4, p. 621, Feb. 2022, doi: 10.3390/ELECTRONICS11040621.
- [33] G. K. Shekhawat and R. P. Yadav, "Efficient Data Sensing Algorithm with Generalized Cascaded Chaotic Maps for Secure Cognitive Radio in 5G Networks," *SN Comput. Sci.*, vol. 5, no. 4, Apr. 2024, doi: 10.1007/S42979-024-02699-3;WEBSITE:WEBSITE:DL-SITE;CSUBTYPE:STRING:PERIODICAL;TAXONOMY:TAXONOMY:ACM-PUBTYPE;PAGEGROUP:STRING:PUBLICATION.
- [34] E. Ozbay, P. K. Bishoyi, and M. Petrova, "Empowering 5G PRS-Based ISAC with Compressed Sensing," Jul. 2024, Accessed: Jul. 02, 2025. [Online]. Available: <https://arxiv.org/pdf/2407.13478>
- [35] H. Liu *et al.*, "Integrated Sensing and Communication Signal Processing Based on Compressed Sensing Over Unlicensed Spectrum Bands," *IEEE Trans. Cogn. Commun. Netw.*, Apr. 2024, doi: 10.1109/TCCN.2024.3391307.
- [36] K. Nayanam and V. Sharma, "Cognitive Radio Based Enhanced Compressive Spectrum Sensing Technique for 5G Adhoc Networks," *Int. J. Sens. Networks Data Commun.*, vol. 13, no. 1, pp. 1–5, Jan. 2024, doi: 10.37421/2090-4886.2024.13.258.
- [37] T. Kanaparthi, R. S. Yarrabothu, and R. Sundar, "Enhancing 5G Massive MIMO Systems Using a Compressive Sensing-Based Approach," *Trait. du Signal*, vol. 40, no. 4, pp. 1705–1713, Aug. 2023, doi: 10.18280/TS.400439.

