Review

Security Challenges in 6G Networks: A Game Theory-based Intrusion Detection with Network Slicing and AI/ML Perspectives

Mantisha Gupta *, Rakesh Kumar Jha *, Manish Sabraj

Posted Date: 16 May 2024

doi: 10.20944/preprints202405.1066.v1

Keywords: 6G; Bandwidth spoofing; Game theory; Intrusion detection system (IDS); ML; Network slicing; Security

Review

Security Challenges in 6G Networks: A Game Theory-based Intrusion Detection with Network Slicing and AI/ML Perspectives

Mantisha Gupta, *IEEE Student Member*, Rakesh Kumar Jha, *IEEE Senior Member* and Manish Sabraj, *IEEE Member*

Mantisha Gupta is with the School of Electronics and Communication Engineering (SoECE), Shri Mata Vaishno Devi University, Katra, Jammu, J&K, India, 182320

Rakesh Kumar Jha is with the Department of Electronics and Communication Engineering, Central University of Jammu, J&K, India, 181143

Manish Sabraj is with the School of Electronics and Communication Engineering (SoECE), Shri Mata Vaishno Devi University, Katra, Jammu, J&K, India, 182320; manish.sabraj@smvdu.ac.in

* Correspondence: mantisha343@gmail.com (M.G.); jharakesh.45@gmail.com (R.K.J.)

Abstract: The vast network of interconnected devices of the Internet of Things poses significant security challenges, necessitating the upgrade of current wireless networks to the 6G standard and an improved intrusion detection system for host networks. Thus this article therefore underscores a game theory concept to analyze the security impediments in wireless communication systems, where a host network bandwidth is jeopardized by the intruder while acting as a legitimate user. While game theory can help with the impending security concerns, network slicing is saliently proposed for large and complicated networks, precipitating a layerwise fragmentation of the concerned network and effectively addressing the security issues in different layers of the IoT framework. However, with increasing network complexity, network security issues incorporating traditional measures become increasingly cumbersome. Therefore, this paper also briefly mentions some of the ML techniques that can be used to classify and segregate valid users from the compromised nodes in the host network. The paper discusses the potential of incorporating intelligence into wireless communication systems to enhance the host network security. The paper further aids in analysing existing security issues in different layers of wireless communication systems, underscoring network slicing for further classification of intruders from user nodes and training the host network using ML/AI per the user application specification.

Keywords: 6G; bandwidth spoofing; game theory; intrusion detection system (IDS); ML; network slicing; security

I. INTRODUCTION

The internet has become an integral part of our lives in the 21st century, providing access to social networking, online shopping, data storage, gaming, online study, and online jobs. However, the internet's widespread use has led to the development of cybercrime, as it has become a significant issue in various spheres of life due to its relative benefits. Hence security has unequivocally been a crucial aspect in present and future wireless communication networks, including B5G and 6G [1]. The IoT, with its growing network of connected devices, further corroborates a serious impediment to data security, tantamountly underscoring the host system's vulnerability [2]. The evolution of wireless communication networks from 1G to 4G, with 5G evolving from mobile broadband to enhanced mobile broadband (eMBB), has been a significant advancement, incorporating the Internet of Things (IoT) for enhanced connectivity [3]. Since 2020, IoT-enabled 5G wireless communication

 doi:10.20944/preprints202405.1066.v1

networks have been deployed globally for massive machine-to-machine communication (mMTC) and ultra-reliable low-latency communication (URLLC) [4].

Furthermore, the testbed experiment reveals that 5G is insufficient for future networks, prompting researchers to explore 6G wireless communication networks, expected to be deployed by 2030 [5]. In contrast to 5G, the 6G wireless communication networks are expected to improve mobile broadband (MBB), expand IoT coverage, and make networks and devices smarter than 5G [6]. IoT connectivity has led to an exponentially growing network of connected devices, making the security of data and its influence on the host system a major concern [7]. Thus, cyberattacks are becoming more subversive, with their arduous behaviours causing a surge in cyber security concerns.

Although 5G is mainly focused on eMBBs, mMTCs and uRLLCs, 6G wireless communication networks are projected to further improve the existing MBBs with enhanced IoT coverage coupled with the intelligence in the networks and devices. As a result, the researchers labelled these upgraded scenarios as further enhanced eMBB (FeMBB), ultra mMTC (umMTC), and enhanced uRLLC (euRLLC) [8]. The technology provides a range of applications, including long-distance and high-mobility communications, alongside communications with very low power consumption. In this way, it is feasible to classify application scenarios like enhanced eMBB/mMTC/uRLLC, with other new elements including space, air, ground, and sea integrated networks, AI-enabled networks, and other similar categories as shown in Figure 1.

AI and big data techniques make it possible to build complex applications. 6G adds new technical standards and performance indicators to meet the needs of these applications, which need fast data transfer, minimum delay, and a reliable network, as illustrated in Table I [9]. Given the usage of terahertz and optical wireless bands, the existing 5G networks are capable of delivering up to 1-10 Tbps of data. AI can enhance network management, increasing area traffic capacity to over 1Gb/s/m^2, spectrum efficiency by 3.5 times, and energy efficiency by up to 10 times compared to 5G technology [10]. Heterogeneous networks, also known as Het-nets, are expected to significantly increase connection density by ten to one hundred, enabling a wide range of communication scenarios and utilizing large bandwidths in high-frequency bands. Mobility will be supported at speeds exceeding $1000km/h$ through ultra-high-speed trains, UAVs, and satellites. Performance criteria such as cost effectiveness, safety capabilities, coverage, and intelligence are also crucial for 6G network evaluation [11].

 doi:10.20944/preprints202405.1066.v1

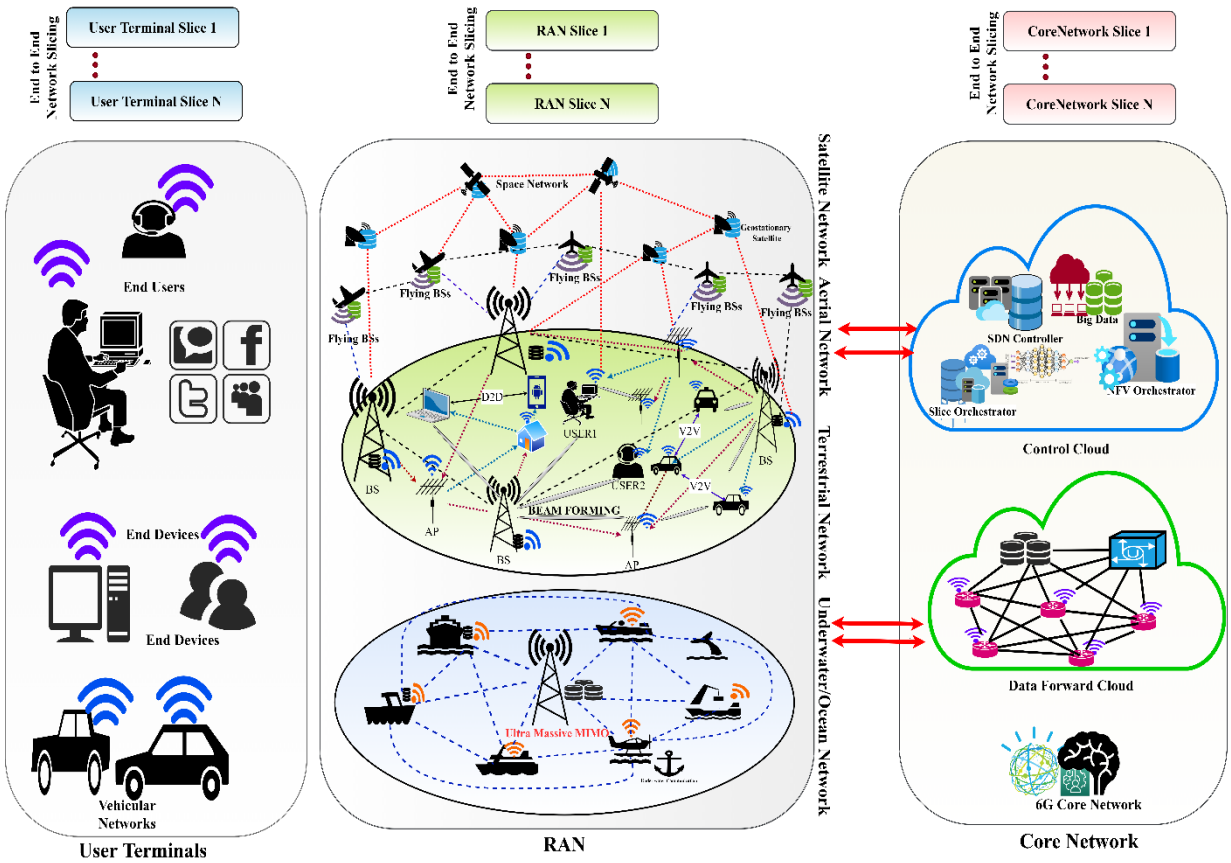

Figure 1. General architecture of slicing different user network scenarios.

Table 1. Comparison of Key Performance Requirements.

Performance attributes	5G	B5G	6G
Data rate	1Gb/s	100Gb/s	1Tb/s
E2E delay	5ms	1ms	<1ms
Radio-only delay	100ns	100ns	10ns
Processing delay	100ns	50ns	10ns
E2E reliability requirement	99.999%	99.9999%	99.99999%

A. Motivation and Contribution

With the widespread adoption of IoT and the erstwhile growing network of connected devices, the security of data and its influence on the host system have been paramount concerns, underscoring that IoT connectivity leads to an exponentially growing network of linked devices. Cybersecurity concerns are thus increasing due to the increasing frequency and complexity of cyberattacks. Therefore, game theory models can be used to predict the future behaviour of intruders, making cyber attacks easier to understand [12].

The main contributions of this paper are as follows:

1. This article implies a game theory for safeguarding the concerned host systems from intrusion attacks in IoT and 6G networks.
2. The paper further illustrates the different security concerns prevailing in the different layers of the contemporary IoT framework.
3. However, in the case of a complex integrated network in 6G, the article mentions the fragmenting or separation of distinct network or application scenarios utilising the network slicing concept before implementing the game theory.

 doi:10.20944/preprints202405.1066.v1

4. With increasing network complexity, network security issues incorporating traditional measures have become debilitatingly cumbersome. Therefore, this paper also briefly mentions some of the ML techniques that can be used to classify and segregate valid users from compromised nodes.
5. Furthermore, as a future aspect, incorporating intelligence into the concerned network requires network training. This in turn enhances the host network's security while simultaneously helping in mitigation and countermeasures against future attacks.

Table 2. Existing Literature Works.

Ref. no	Year	Research title	Technology used	Algorithm used	Performance Indicators	Inference
[13]	2018	Hap-SliceR-A radio resource slicing framework for 5G.	Virtualised radio resource slicing strategy.	Heuristic algorithm for resource allocation with RL.	• Slice Reservation Index(SRI) • Round Robin(RR) and Best channel quality indicator (BCQI) for UL/DL data rates.	• A feasible 5G network solution that is implemented in a standard cloud computing infrastructure near the RAN edge.
[14]	2019	Intelligent resource scheduling strategy (iRSS) for 5G RAN slicing.	The framework is a combination of Deep Learning and Reinforcement Learning.	LSTM-RNN is used as a DL algorithm and A3C as an RL algorithm.	• DL for large-scale resource allocation. • RL for online resource scheduling to manage small-time-scale network dynamics.	• Resource scheduling for improving multiplexing gain, meeting RAN slicing requirements, and addressing issues like inaccurate predictions and unexpected state changes.
[15]	2020	ML for resource management in cellular IoT networks	ML-DL in Hetnets, MIMO, and D2D communications.	ML and DL-based techniques for resource management.	• Cellular, Low power, cognitive and mobile IoT networks. • Optimization, heuristic and game theoretic approaches.	• It covers resource management techniques such as scheduling, duty cycling, clustering, data aggregation, traffic classification, prediction, power allocation, and interference management.
[16]	2021	Intelligent resource slicing for eMBB and URLLC for 5G/B5G	Resource slicing in dynamic multiplexing scenarios of URLLC and eMBB services of 5G.	DRRA-PGACL is utilized for efficient resource allocation in eMBB and URLLC scenarios.	• DRRA in eMBB resource allocation for low computational complexity. • URLLC scheduling employs DRL as PDACL to maintain latency and reliability.	• The eMBB focuses on maintaining a high data rate while adhering to URLLC reliability constraints, with the DRL approach facilitating a good convergence rate.
[17]	2021	Multi-agent reinforcement learning (MARL)	MARL in Markov, stochastic games and extensive forms of games.	Dynamic programming, game theory, optimization theory and statistics.	• MARL is used in applications like autonomous driving and robotics.	• MARL frameworks can be centralized, decentralized with networked agents, or fully decentralized.
[18]	2021	ML-based physical layer security	ML is used to reduce the increasing	ML applied to wireless physical layer security (WPLS)	• Relay node selection, antenna selection and authentication with ML	• ML is utilized in various WPLS networks such as IoT, D2D, cognitive radio, and UAV.

 doi:10.20944/preprints202405.1066.v1

			complexity of wireless networks.			
[19]	2022	PSARE: Online participation selection scheme for area coverage ratio	Area coverage ratio in Mobile Crowdsensing using RL	Q-Learning for online participation selection	• Coverage degree, coverage quality and time complexity.	• The framework utilizes RL with a Q-learning-based online participation selection scheme to enhance coverage ratio and degree.
[20]	2022	Optimised packet forwarding in multi-band relay networks	Enhancing network coverage using relay packet forwarding.	Q-learning and Markov decision process (MDP)	• Packet transmission time, buffer overflow and effective throughput	• The framework utilizes multiple relay nodes as MDP to create an efficient channel allocation algorithm.
[21]	2023	Adversarial attacks and defences in ML network	Counter-attack detection and network robustness enhancement using ML	ML and deep neural network (DNN)	• New types of attacks include search-based, decision-based, physical world attacks, and hierarchical classification attacks.	• The latest defence methods balance training costs with performance, maintain clean accuracy, overcome gradient masking, and ensure method transferability.
This paper	2024	Network slicing enabled security concerns in 6G	Intrusion detection system (IDS) using game theory	Game theory integrated with Network slicing and ML	• IDS implementation using game theory in path loss models for different user scenarios. • Network slicing and ML for intrusion detection in large and complex networks.	• The IoT significantly impacts data security, necessitating updates to B5G and 6G wireless networks and changes in communication systems for robust authentication and trust mechanisms.

The paper aims to integrate game theory and machine learning with the network slicing concept to enhance security in 6G systems. To protect against future attacks, this can be used effectively in the upcoming intelligent wireless tactile and touch-based user application systems interfaced with the augmented and virtual reality (AR/VR) infrastructure. Game theory and network slicing can thus be used in both the physical network and the backbone network [22]. Various state-of-the-art literature works concerning network slicing, intelligence, and security aspects of IoT-enabled 6G systems are summarised in Table II and illustrated in the subsection below.

B. Existing Works in Security involving Network Slicing and Machine Learning

The research in [13] proposes a Hap-SliceR, which is a network-wide radio-slicing strategy that uses reinforcement learning to virtualize radio resources, allowing for novel customization through a low-complexity heuristic resource allocation algorithm for haptic communication. The authors in [14] address challenges in resource scheduling in RAN slicing, such as performance isolation, diverse service requirements, and network dynamics. They propose an intelligent resource scheduling strategy (iRSS) using deep learning and reinforcement learning, adjusting the significance between prediction and online decision modules based on traffic data.

The research in [16] proposes a resource-slicing problem to maximize the eMBB user average data rate while minimizing variance, using URLLC constraints and the policy gradient-based actor-critic learning (PGACL) algorithm for reliable resource allocation, addressing network traffic and channel variations. Machine learning and deep learning models are promising for automatic resource management and decision-making in complex IoT environments, re-tuned with environment changes, and are further being explored for complex radio resource management problems [15].

 doi:10.20944/preprints202405.1066.v1

The research in [18] highlights security challenges in the intelligent wireless physical layer system (WPLS) for applications like the Internet of Things (IoT), device-to-device (D2D), cognitive radio(CR) and unmanned aerial vehicles (UAV). The study in [19] explores the issue of online participant selection in urban data sensing and collection, aiming to improve coverage quality in mobile crowdsensing using RL and Q-learning approaches.

Relay-based networks are increasingly utilized in device-to-device and dronecell networks for enhanced capacity and coverage, utilizing MDPs to assess performance metrics like transmission time, buffer overflow, and effective throughput [20]. The research findings in [21] demonstrate that adversarial assaults have the potential to exploit vulnerabilities in machine learning and deep neural network-based algorithms, namely in the domains of wireless signal categorization, modulation scheme detection, and MIMO network resource allocation.

C. Paper Structure and Organization

The paper is organized as follows. The paper discusses the 6G wireless communication system, its security aspects, network slicing, and state of art machine learning implementation in Section I. It also addresses security concerns in key technologies in Section II, while Section III addresses various security threats in different layers of the IoT framework and discusses the role of UAVs in the IoT framework, game theory approach for intrusion detection, and existing network interfacing with other access systems. The proposed network scenario with its system model and its mathematical implementation is discussed in Section IV.

Section V comprises the flow process for the suggested system while Section VI further delves into corroborating network slicing and machine learning for intrusion detection in a layered IoT framework and to classify the valid users from the compromised nodes. Section VII comprises the simulated results incorporating the intrusion detection system for the suggested scenario while discussing the security countermeasures, challenges, and research directions for B5G and 6G networks, and the paper concludes in Section VIII.

II. Security Concerns in 6G Network

Wireless mediums are subject to data intrusion assaults, hence B5G/6G-based IoT networks need to limit radio jamming attacks to guard against such attacks [23]. Control channel and data channel attacks are intelligent jamming methods in wireless systems that cause packet transmission and reception failure over data channels [24]. The potential security risks associated with intelligent Tactile-based Internet of Things (IoT) systems, namely those including touch-based infrastructure in the context of 6G technology, are present across several stages of data processing. These stages include data collection, information filtering, data fusion, representation modelling, processing, and interpretation [22], [25]. IoT systems have several security concerns, such as terminal security, data transmission security, data processing security, and management security.

Terminal security prevents unauthorized access to devices, while data transmission security protects against theft or loss during data transmission. Data processing security safeguards personal information from disclosure and management security ensures the scalability of security measures [26]. Privacy breaches in WIFI networks can be caused by Smart Device usage, position-based services, and insufficient user knowledge, necessitating the development of new methods to protect these systems [27].

Therefore, at this juncture, the privacy of IoT data synergically travelling via the concerned network has a critical exigency for IoT networks owing to the huge scale and scattered nature of the IoT networks. Some of the key technologies enabling security and privacy in IoT and the 6G system are mentioned below:

A. Blockchain

New content-oriented networks, due to their high cost and complexity, may not fully control data, exposing users' personal information if not secured. To protect the underlying personal

 doi:10.20944/preprints202405.1066.v1

information in 6G networks, strong access control and encryption techniques are needed especially in highly interactive applications like tactile and touch-based IoT applications. The blockchain-based multilayer model is expected to improve local coordination of IoT equipment, reduce computational and network load, and provide a secure and reliable IoT network with contract records in multiple blockchains [28].

B. Edge/Fog Computing

Edge/Fog computing is a promising approach that extends cloud computing capabilities to the network edge, improving processing, data storage, communication, and networking. It offers reduced latency, improved mobility support, enhanced location awareness, and the ability to deploy applications across geographically distributed locations. Maintaining trust between IoT devices and fog nodes is crucial due to potential device malfunctions or malicious attacks, as fog nodes validate the authenticity of service-seeking devices. Additionally, Fog nodes close to the end user may capture information like their location, identity, and utility usage, which might make privacy challenging to preserve in those nodes compared to cloud computing nodes [29].

C. Software Defined Networking (SDN)

SDN has the potential to considerably simplify network management and control, as well as to improve the security and privacy of the tactile/touch-based IoT applications in the 6G system. Moreover, the separation of the data plane and control plane poses challenges for unauthorised individuals attempting to get data, even in the event of successful access to the data plane. SDN also aids in the automatic detection of a malware-affected endpoint or network segment. Essentially, adding permitted flows to IoT networks while authenticating IoT devices is what has been most commonly used to protect IoT networks from fraudulent devices and assaults [30].

D. Machine Learning

Machine learning (ML) approaches, such as supervised, unsupervised, and reinforcement learning, have been used in many applications, including access control, authentication, spyware detection, and anti-jamming offloading. Traditional machine learning methods may not be suitable for IoT devices with limited resources, such as computer processing power, radio and energy resources, device quality variations, dependable low-latency training outputs, and devices with different capabilities. In this regard, it is vital to research creative authentications on learning, access control, and secure downloading/storage of tactile/touch-based IoT devices, to prevent assaults like physical and media access control (MAC) layer attacks, jamming, smart attacks and eavesdropping [31].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2024 doi:10.20944/preprints202405.1066.v1

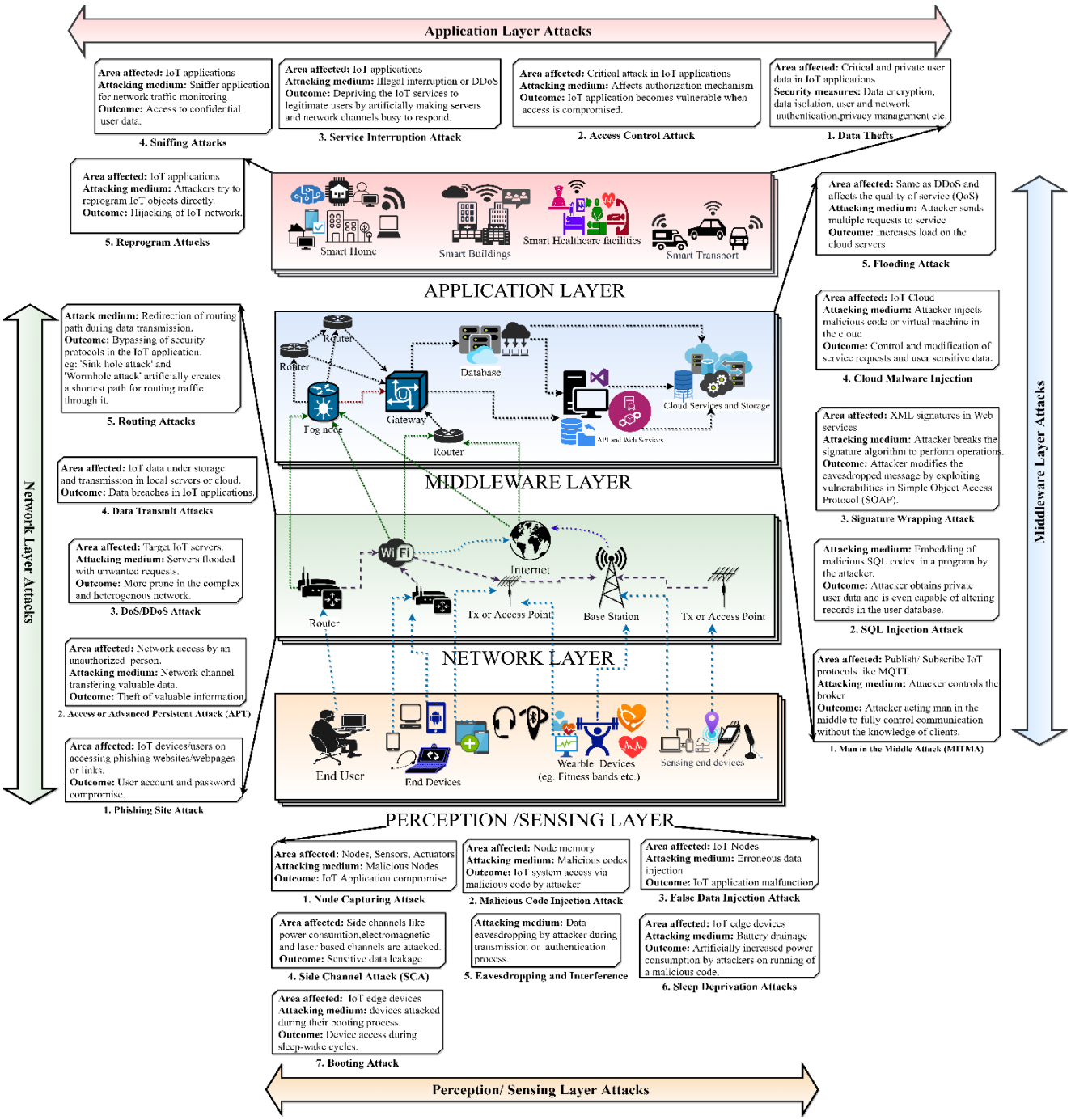

Figure 2. Potential security threats in various layers of IoT interface.

III. Security Aspects to be considered

Security is essential when using mobile IoT devices (like UAVs and bot devices) in highly interactive environments, such as the Tactile interfacing environment. Some of the important security aspects that must be taken into consideration are listed below and are effectively illustrated in Figure 2 using a layerwise IoT interfacing architecture. The security of the IoT perception layer is susceptible to several types of security attacks, such as node capture, code injection, side channel assaults, eavesdropping, interference, and booting. These security vulnerabilities provide substantial risks to the overall security of the IoT network. The networking layer is vulnerable to several forms of attacks, including routing assaults such as sinkhole and wormhole attacks, attacks on data transfer, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks and Phishing site attacks IoT middleware provides powerful computation and storage by abstracting the network and application

 doi:10.20944/preprints202405.1066.v1

layers. It consists of brokers, persistent data storage, queuing systems, and machine learning. Middleware security issues fall mostly on database and cloud security [37]. Despite its usefulness in providing reliable IoT applications, middleware is susceptible to attacks that can control the entire application, which include flooding attacks, cloud malware attacks, man-in-the-middle attacks, SQL injection attacks, and signature wrapping attacks. While, the application layer encompasses various types of threats, such as data theft and access control attacks, service interruption attacks, sniffing attacks, and reprogramming attacks.

Table 3. Machine Learning Implementations in Real-Time Wireless IoT Networks.

Source	Machine Learning Algorithms	Network Optimisation Entity	Use cases in IoT network
[32]	Classification	Data Prediction, Time Prediction, Labelling data detection	Smart Traffic, Smart Cities
[33]	Clustering	Prediction and data segregation, Passenger data pattern	Smart Traffic, Smart Health
[34]	Anomaly detection	Finding anomalies in power datasets, Fault detection	Smart Traffic, Smart Environment
[35]	Support Vector Machine(SVM)	Data Forecasting	Smart Weather prediction
[36]	Linear Regression	Real-time prediction and data reduction	Economics, Market analysis, Energy usage

A. UAVs in IoT Network

UAVs are increasingly utilized in precision agriculture, irrigation management, crop health monitoring, and cattle herding. They enhance data transmission and security by connecting with base stations and vehicles. UAVs also facilitate package delivery to customers' doorsteps due to safe flight control and wireless communication. They are also used in search and rescue operations, considering data and QoS requirements, adaptability, safety, and user privacy [38]. Traditionally, deploying UAVs in wireless systems faces challenges like channel models, dynamic cell associations, and energy constraints.

The ongoing research avenues concerning UAVs, V2V and other IoT D2D networks are in image processing, deep learning, mobile edge computing (MEC) [39], fog, and cloud computing [40]. As UAV deployment increases, new challenges arise in multi-agent systems like trajectory, resource allocation, and user association. Game theory can help solve these problems using concepts like Nash or correlated equilibrium, analyzing the interaction between agents in a communication network [41]. The increasing number of V2V and UAV devices necessitating complex tasks may render traditional game-theoretic algorithms ineffective. A potential solution is to employ machine learning techniques like function approximation, policy gradient, and multi-agent actor-critic [42].

B. Interfacing Existing Network with other Access Systems

Wireless communications are diverse technologies, services, and applications suited to specific deployments and user environments, categorized by content, services, frequency bands, standards, data rates, delivery mechanisms, mobility, and cost [43]. Updating technologies aim to offer diverse mobile telecommunication services across different teledensities and geographic areas, especially in developing countries where low population density, teledensity, and income levels hinder access to mobile communication [44]. Satellite networking offers extensive geographical coverage, enabling services in low-population regions like rural and desert areas, and marine and aeronautical settings, and serves as a valuable supplement to terrestrial networks [45]. It lowers entry costs and brings telecommunications to those with mobile or fixed-line telephones, benefiting from limited system complexity.

 doi:10.20944/preprints202405.1066.v1

The terrestrial component could expand geographic coverage through lower frequency ranges or satellite components, but market conditions may limit this. Maintaining 6G service regions beyond 5G is critical for achieving user expectations given that globally harmonised frequencies may provide low-cost services to rural and low-income communities, decreasing terminal complexity and system costs [46]. 5G systems offer diverse services like symmetrical, asymmetrical, and unidirectional, managing different QoS levels for efficient packet-based transport. They enable nomadic and mobile wireless access to multimedia services, with 5G-NR interfaces capable of handling various data rates, ranging from 100 MB/s for high mobility to 1 GB/s for low mobility [47].

The data rates of radio interfaces are affected by a variety of variables, including traffic characteristics, service specifications, deployment situations, spectrum availability, and interference circumstances. The next-generation system should be designed to complement different access technologies for different service requirements and environments, providing a flexible service platform and promoting widespread adoption of products, services, content, ease, and efficiency [48]. A personal digital assistant offers global mobile access, high security, and personalized multimedia services. Adaptive packet data transfer solutions are crucial for integrating services in packet-based applications and networks, supporting asymmetric traffic and incorporating technologies like cellular, radio LAN (RLAN), digital broadcast, and satellite [49].

The seamless interaction of various systems is crucial for users to receive diverse content. The flexible core networks connect different radio access systems, allowing users to access desired networks and services. Horizontal and vertical handoff, service provision, mobility, security, and QoS management are essential requirements. This enables an "optimally connected anywhere, anytime" network with interoperable access systems connected to a packet-based core network[50].

Access systems can be hierarchically organized, similar to cellular structures in mobile radio systems, and can be utilized across various applications and radio settings. The access systems interact via vertical handover or session continuation, which involves service negotiation to accommodate candidate system applications [51]. The system consists of layers like distribution, cellular, hotspot, personal network, and fixed or wired. Distribution distributes information via uni-directional links, cellular consists of multiple cell layers, hotspots for high data rate applications, and personal networks for short-range direct communication.

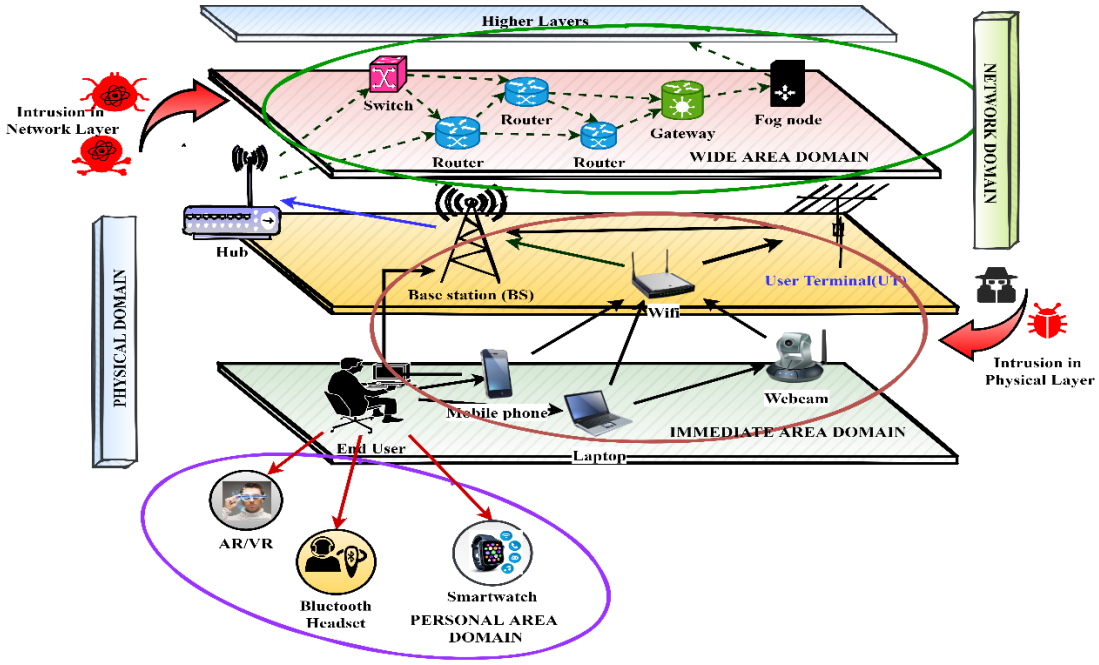

Figure 3. System model for a security breach in sliced physical and network domain in IoT wireless network.

 doi:10.20944/preprints202405.1066.v1

The article further explains the network entities and channel modelling in the 6G communication systems, which also include the control plane and user plane latency [52]. Control plane latency is the idle-to-active time, omitting forward link, paging, and wireline networking signal delays. The one-way transit time between an SDU packet and a protocol data unit (PDU) is user plane latency. Advanced 6G network interfacing involves layer 3 and above communication in physical and network domains, forming a backbone system for edge communication, as discussed further.

1. Cell Spectral Efficiency (η) is the number of correctly received bits in service data units (SDUs) delivered to layer 3 over time, calculated by dividing aggregate throughput by channel bandwidth and the number of cells.
2. Peak Spectral Efficiency is the highest theoretically evaluated data rate for a single mobile station under error-free conditions, excluding resources for physical layer synchronisation, reference signals, guard bands, and guard times.
3. Optimal network bandwidth is determined by various factors including RF bandwidth, duplex technique, network efficiency, traffic models, QoS requirements, spectrum efficiency, adaptive antennas, and MIMO [53].
4. The control plane latency should be less than 100 ms to establish the user plane and ensure a smooth transition from idle to active.
5. User plane latency, also known as transport delay, refers to the delay caused by protocols and control signalling during the transportation process, assuming the user terminal is active.

IV. Proposed Network Scenario

The given section proposes a system model illustrating a security breach in the sliced and interfacing physical and network domains of the host network, with its system model and problem formulation.

A. Proposed System

Figure 3 presents an intrusion detection system divided into physical and network domains, comprising the personal area domain, immediate area domain and a wide area domain. The personal area domain here involves direct communication between user terminals and peripheral devices, while the immediate area domain covers communication between devices within the user environment. The wide area domain includes communication between devices via network operator infrastructure, covering a range of a few meters to several tens of meters. The network is sliced into different domains using network slicing, with each layer having its own independent yet interconnected network. All of these layers are susceptible to security attacks. Therefore, the suggested system model proposes to use game theory to address intrusion detection in a low-complexity host network. However, to address security breaches in a highly complex network domain, network-slicing and game theory are proposed. Moreover, to train the concerned network against similar breaches in the future, ML approaches must be corroborated using the network complexity to prevent future breaches.

 doi:10.20944/preprints202405.1066.v1

Table 4. Channel Parameters in 6G Wireless Network.

S.no						
1.	$\sum \mathcal{B}_{\text{(More bandwidth access)}}$	Millimetre wave (mm-wave)[54]	Terahertz (THz) network[55]	Optical wireless communication[56]	Cognitive Radio Network (CRN)[57]	Full Duplex (FD) and multi-standard systems[58]
2.	$\sum \mathcal{P}_{\text{(More Power and efficiency)}}$	Small cells and cell-free networks [59]	Green communication[60]	Advanced modulation and Network coding[61]	Polar codes, Turbo codes[62]	Low-density parity check code (LDPC)
3.	$\mathcal{N}_{\text{noise and filtering}} + \mathbb{I}_{\text{interference}}$	Interference randomisation[63]	Interference coordination [64]		Interference cancellation[65]	Interference alignment[66]
4.	Applications	Industrial IoT[67]	Augmented, Virtual and Mixed reality (AR/VR/MR)[68]		Wearable displays	Robots and Drones

B. System Model

We consider a wireless channel with $\mathbb{N}$ deployed nodes, where the majority of connected nodes are legitimate users. The reason for such an assumption is to propose a model to check the effect of a few eavesdroppers or attackers on the majority of the legitimate users that are connected to the same base station. Whereas some of the nodes in the network might be either compromised nodes or intruders trying to access the host network. Let there be 'i' number of legitimate users and '$\mathbb{N} - i = j$' number of attackers accessing the host network, with P_n being the transmission power by the base station (BS) to each connected device, either user or attacker. Here, as per the proposed scenario, both the legitimate user and the attacker compete with each other to try to gain access to the same host network.

We consider (x_{BS}, y_{BS}) to be coordinates of the connected BS. Let us represent (x_U^i, y_U^i) and (x_A^j, y_A^j) as the coordinates of the corresponding i^{th} user and j^{th} attacker located at a certain distance d_{BS-i} and d_{BS-j} from the BS serving the host network. The distance between the BS and the user/attacker is computed by

$$d_{BS,i} = \sqrt{(x_{BS} - x_U^i)^2 + (y_{BS} - y_U^i)^2} \tag{1}$$

and

$$d_{BS,j} = \sqrt{(x_{BS} - x_A^j)^2 + (y_{BS} - y_A^j)^2} \tag{2}$$

However, it is assumed that the connected BSs are well equipped with omnidirectional antennas, with known CSI at both the transmitter and receiver sides. Here the connected user or attacker is denoted by U and A respectively in a Rayleigh Flat fading channel. Furthermore, a constant noise power is assumed at every instant for the i^{th} user and j^{th} attacker. Based on the given assumptions, the concerned BS transmits the signal $\boldsymbol{x}_i$ to the i^{th} user, and the signal received at the receiving end is given by

$$y_i = \boldsymbol{h}_i \boldsymbol{x}_i + n_i \tag{3}$$

here $n_i \sim \mathrm{N}(0, \sigma_m^2)$, denotes the complex additive white Gaussian noise (AWGN), having zero mean and variance σ_m^2 at the receiving node, and $\boldsymbol{h}_i$ is the Rayleigh fading coefficient associated with the channel between the host BS and the valid user. α denotes the path loss exponent of the main channel. Likewise, (3) can be further written as

$$y_i = \sqrt{P_n d_{BS,i}^{-\alpha}}\, \boldsymbol{h}_i \boldsymbol{x}_i + n_i \tag{4}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2024 doi:10.20944/preprints202405.1066.v1

The attacker on the other hand pings the host network and tries to eavesdrop on the signal between host BS and the users and receives the following signal:

$$z_j = \boldsymbol{h}_j \boldsymbol{x}_j + n_j \quad (5)$$

where $\boldsymbol{h}_j$ is the channel coefficient between j^{th} attacker node and host BS, and n_j denotes the complex Gaussian noise with zero mean and σ_m^2 variance.

Following this the received signal at i^{th} user is further expressed as a combination of actual signal components, AWGN noise and interference from neighbouring nodes which may either be compromised nodes or intruders.

$$|y_i|^2 = P_n {d_{BS,i}}^{-\alpha} |\boldsymbol{h}_i|^2 |\boldsymbol{x}_i|^2 + \sigma_m^2 + \sum_{j=1, j\neq i}^{n} P_j \, {d_{BS,j}}^{-\alpha} \left|\boldsymbol{h}_j\right|^2 \left|\boldsymbol{x}_j\right|^2 \quad (6)$$

here P_j represents the transmission power allocated to the interfering j^{th} node, which may be either an attacker or a failed node.

The proposed scenario involves the attacker preparing to attack the host network by analyzing the SINR values in the interfering network regions. Therefore the signal-to-noise plus interference ratio (SINR), is crucial in evaluating the intrusion level in the received signal, as shown

$$SINR = \frac{Signal\ power(P_S)}{Noise\ power(\mathcal{N}) + Interference\ between\ nodes(\mathbb{I}) + Interference\ due\ to\ intrusion\ on\ host\ network(\delta)} \quad (7)$$

The overall SINR comprises the ratio of the transmission power by the host network, which is denoted as signal power P_s, to the combined noise power $\mathcal{N}$ of all the connected entities in the host network including both legitimate users and intruders, with '$\mathbb{I}$' as the nodal interference between connected entities in the host network. However, due to an intrusion attack, the SINR taken into consideration also comprises the interference occurring due to an intrusion attack on the concerned host network. The received instantaneous SINR at the i^{th} user can be mathematically expressed as:

$${\gamma_i}^t = \frac{P_s}{\sigma_m^2 + \sum I} \quad (8)$$

where $P_s = P_n {d_{BS,i}}^{-\alpha} |\boldsymbol{h}_i|^2 |\boldsymbol{x}_i|^2$, thus (8) can be further rewritten as

$${\gamma_i}^t = \frac{P_n {d_{BS,i}}^{-\alpha} |\boldsymbol{h}_i|^2 |\boldsymbol{x}_i|^2}{\sigma_m^2 + \sum_{j=1, j\neq i}^{n} P_j {d_{BS,j}}^{-\alpha} \left|\boldsymbol{h}_j\right|^2 |\boldsymbol{x}_j|^2} \quad (9)$$

Here σ_m^2 is the noise power and all channels are assumed to be available including those for the attacker. Therefore the average channel capacity of the i^{th} user can be expressed by

Table 5. List of Symbols used.

Symbol	Description
$d_{BS,i}$	Base station-User link
$d_{BS,j}$	Base station-Attacker link
P_n	Reference channel power allocated by the BS to each connected user/attacker.
$\boldsymbol{h}_i,\ \boldsymbol{h}_j$	Channel coefficient vector from BS to the i^{th} user and j^{th} attacker respectively.
γ_i	SINR at receiver signal.
α	Pathloss exponent of the main channel.
σ_m^2	Noise power
B_n^t	Total bandwidth allocated to n users at instant t
$\mathcal{T}_i^t$	Average throughput of i^{th}user accessing BS at instant t
$\acute{C}_{sec}$	Secrecy capacity
$\acute{C}_i$	Channel capacity before intrusion attack
$\acute{C}_j$	Channel capacity after intrusion attack
δ	Signal interference due to intrusion
$\mathcal{N} + \mathbb{I}$	Overall noise and interference in the established channel
$\acute{U}_{User}$	A valid or legitimate user
$\acute{U}_{Attacker}$	Attacker or intruder gaining host bandwidth access
$\mho_{user}$	Set of strategies adopted by the valid user.
$\mho_{attacker}$	Set of strategies by attacker accessing the host bandwidth
ϕ_i^1	Strategy played by the user

 doi:10.20944/preprints202405.1066.v1

ϕ_j^2	Strategy played by the attacker element
(a'_{ji}, a_{ji})	Rewards earned by user and attacker during the game played.

$$\acute{C}_i = \log_2(1+\gamma_i{}^t) \text{ bps/Hz} \quad (10)$$

As per the required scenario, the total bandwidth B_{Total} is allocated to each connected node in the considered network. Initially, equal bandwidth access is granted to both the users and attackers in a suggested host network, where bandwidth obtained by each connected device at t time slot is estimated by:

$$B_n^t = B_{total} f(n^t) \quad (11)$$

The total bandwidth accessed is, hence a function of the total n number of connected entities (users and attackers) at instant t, as per the network deployment.

In due course, both the user and the attacker try to gain access to the majority of the host bandwidth, each of them corroborating their set of strategies while playing a game. The game theory concept is therefore implemented in the proposed scenario for network monitoring, detecting intruder elements, and removing malicious attacker devices from the network, thereby preventing their access to the host network [69].

The primary goal is to safeguard host network data from unauthorized access and prevent future incidents by analyzing channel capacity in real-time scenarios, as illustrated in Table IV. Table V provides a comprehensive description of the notations utilized in the system model.

C. Problem Formulation

This section focuses on detecting intrusions on the host network after an intruder breaches host security and attempts are made to recover the data lost during the attack. The system evaluates the level of intrusion by assessing the channel capacity, which is determined using the Shannon capacity theorem. Hence the average throughput of an i^{th} connected user to the BS at instant t is given by:

$$\mathcal{T}_i^t = B_n^t \log_2(1+\gamma_i{}^t) \quad (12)$$

This is applied in the concerned scenario where an attacker is present among network users but not authorized to access the host network compared to the user. Therefore from (10) and (11), the secrecy capacity for the given setup may be evaluated as:

$$\acute{C}_{sec} = \begin{cases} \acute{C}_i - \acute{C}_j, & \gamma_i^t > \gamma_j^t \\ 0, & \text{otherwise} \end{cases} \quad (13)$$

here γ_i^t and γ_j^t are the instantaneous SINR at the user and attacker respectively. Using (13), the overall channel capacities of the host network in the proposed scenario, before and after the intrusion activity are illustrated as:

$$\acute{C}_i = \log_2\left[1 + \frac{P_n d_{BS,i}{}^{-\alpha} |\boldsymbol{h}_i|^2 \, |\boldsymbol{x}_i|^2}{\sigma_m^2 + \sum_{j=1, j\neq i}^{n} P_j d_{BS,j}{}^{-\alpha} |\boldsymbol{h}_j|^2 |\boldsymbol{x}_j|^2}\right] \quad (14)$$

(Before Intrusion)

$$\acute{C}_j = \log_2\left[1 + \frac{P_n d_{BS,i}{}^{-\alpha} |\boldsymbol{h}_i|^2 \, |\boldsymbol{x}_i|^2}{\sigma_m^2 + \sum_{j=1, j\neq i}^{n} P_j d_{BS,j}{}^{-\alpha} |\boldsymbol{h}_j|^2 |\boldsymbol{x}_j|^2 + \delta}\right] \quad (15)$$

(After Intrusion)

Here $\delta = \sum_{j=1, j\neq i}^{n} P_j \, d_{i,j}{}^{-\alpha} |\boldsymbol{h}_{i,j}|^2$, which denotes the interference due to an intrusion attack on the host network, while $\boldsymbol{h}_{i,j}$ denotes the channel coefficient between the i^{th} and j^{th} node. Hence,

$$\acute{C}_j \leq \acute{C}_i \quad (16)$$

Equation (16) indicates that the overall channel capacity post-intrusion is less than the total channel capacity before the intrusion into the host network.

Since all the concerned parameters are the statistics of SNR, the interference due to intrusion decreases the system SNR thus affecting the channel capacity and ultimately reducing the overall throughput of the host system. The system thus requires an effective intrusion protection system to restore channel capacity after data loss and enhance the system throughput. Game theory is thus incorporated in the suggested system, increasing the SNR of the valid user, and leading to improved

 doi:10.20944/preprints202405.1066.v1

channel capacity of the system. Thus as per the system model, more bandwidth is allocated to the valid user, thereby enhancing the system throughput, and preventing attacks on the host network bandwidth.

Furthermore, the research in [70] examines B5G/6G wireless communication networks, focusing on application scenarios, performance measurements, and key technologies. It covers mm-wave, terahertz, optical wireless channels, HST, V2V, MIMO, OAM, and IoT, with AI optimizing network performance. The proposed scenario aims to create a secure, robust network, ensuring security for both physical and network layers, contrasting with 1G-5G methodologies that focus only on network setup and operation. The following section presents the flow process for the proposed system model and network scenario, as previously discussed.

V. Flow Process and Implementation

The proposed scenario implementation is illustrated in Figure 4, starting with resource allocation, which involves initializing and assigning input parameters in the host network model, such as channel conditions, channel gain, and power of the connecting base station. The research aims to enhance network security by monitoring user behaviour and intruder nodes, and potentially removing suspected attacker nodes. The system addresses security concerns by detecting intrusions and removing compromised nodes. Here, game theory is applied in this scenario where both the user and attacker engage in a game to gain more network bandwidth, starting with their strategies and rewards depicted through the prisoner's dilemma (PD) matrix [71].

During network initialization, the host system allocates bandwidth to connected users, with valid users receiving a larger share than attackers. The system uses channel modelling to allocate bandwidth to connected valid users and intruders, with the user receiving a larger share due to their authenticity with the host network. It therefore compares the SNR or SINR values of both the attacker and user and grants access to the one with a higher SNR value. The game theory thus allows both valid users and attackers to access the host network bandwidth.

The attacker adapts to the host network over time, proving the current strategy ineffective in preventing host bandwidth spoofing after repeated monitoring and analysis. After studying the network, the attacker eventually obtains a higher signal-to-noise ratio than the authenticated user, thus gaining full access to the host bandwidth. The attack focuses on the output channel capacities and involves access to the entire host bandwidth. Furthermore, in sparsely deployed networks, intruder nodes may not be immediately eliminated despite broadcasting large messages or refusing packet forwarding, leading to unstable communication; however, they may eventually return to a normal state.

If a node continues to exhibit malicious behaviour, it will be labelled as an attacker and immediately removed, based on the game theory concept. Implementing a protection mechanism is hence crucial for detecting and regulating unauthorised intrusions into the host network, thereby ensuring protection against future security threats. The protection mechanism follows a similar game theory approach to eliminate malicious nodes by initializing all active users, identifying recent bandwidth-assigned users, and creating a detailed datasheet. The network ensures system validity by including only the authentic users and detecting the intruding elements, in that way restricting their access to system data.

The system detects network intrusions and denies unauthorized access to the host database by verifying user access through cross-verification and authenticity and comparing their SNR values with the previous database. The host system then adjusts its security algorithm, removing an intruder from its database and assigning bandwidth to the legitimate user, thereby ensuring network security. The paper analyzes user densities and data rates in various scenarios to evaluate attack and protection models for reducing bandwidth spoofing in networks.

The system therefore considers three scenarios before, during, and after data intrusion in the host network in the simulated results. The protection mechanism detects and overcomes intrusions by restoring the original signal without intrusion. However, the output capacity after recovery is slightly less, indicating information loss during an intrusion attack.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2024 doi:10.20944/preprints202405.1066.v1

A. Game Theory Approach

Game theory is a field that studies strategic interactions among rational players, focusing on optimizing their benefits. It offers efficient and robust distributed algorithms, making it useful in wireless networks for modelling, analyzing, and designing distributed schemes. Hence in this aspect, game theory is utilized to study and forecast the future behaviour of the complicated attacks in present and future networks. Furthermore, it aids in the characterization of the intricate nature of these attacks and facilitates the prediction of their future patterns, hence enhancing the ability to assess and prepare for effective responses.

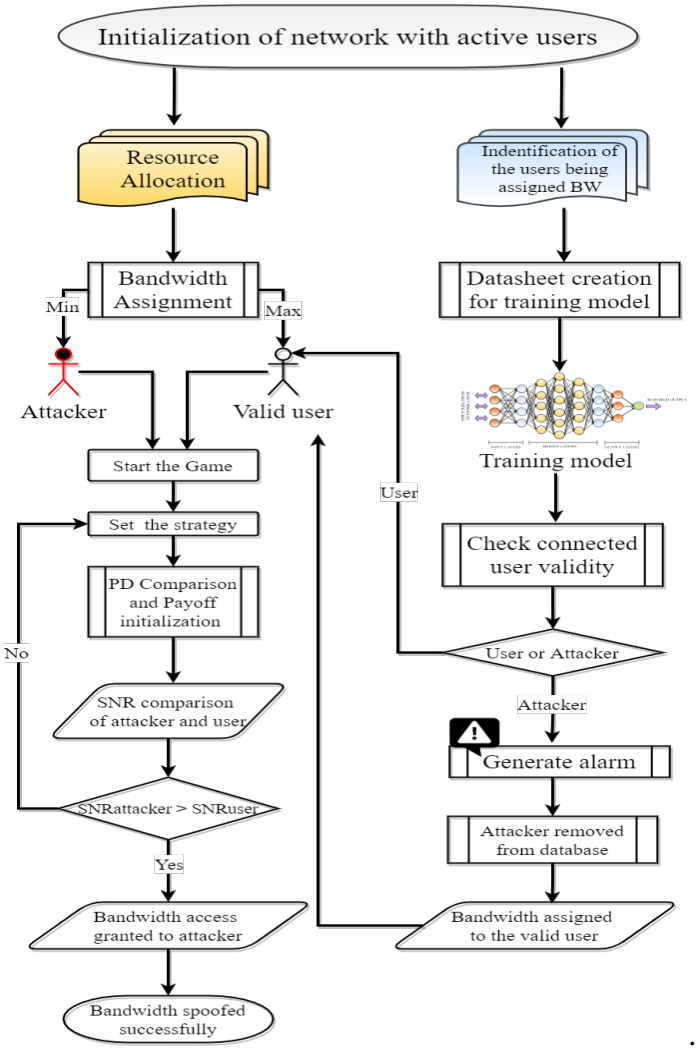

Figure 4. Flow process of the proposed system.

The wireless network components commonly seen in contemporary settings encompass vehicle ad hoc networks (VANETS)[72], drone networks, and high-speed trains (HST)[73]. These components consist of a combination of mobile and stationary nodes, each equipped with a range of communication technologies and infrastructure. Intrusion detection systems (IDS) are used to safeguard networks from both internal and external cyber threats. The IDS employs anomaly detection policies to identify malicious activities perpetrated by attackers. However, these policies are vulnerable to many forms of attacks, such as location spoofing. The accurate prediction and detection of zero-day threats, which encompass one or two intricate attacks, can be achieved through the utilization of Game Theory and Machine Learning (ML) methodologies [74], some of which are illustrated in Table III.

A game consists of three elements: the set of players N, the strategy space for each player ϕ_i, and the payoff $\mathcal{U}_i$, which is the reward players receive at the end of the game based on other players'

 doi:10.20944/preprints202405.1066.v1

actions. The wireless communication network involves players like UAVs, end devices, ground users, or base stations, where the strategies may include beaconing, offloading, channel assignment, and intruder evasion. While the payoffs comprise throughput, SINR, delays, and node coverage based on the real applications. A game is static if all players make decisions simultaneously without knowing each other's strategies, while it is dynamic if players make decisions sequentially or repeatedly[69].

Games can be categorized into complete and incomplete information games based on their known information structure. The information games are perfect or imperfect based on whether all players know each other's historical actions. Cooperative games are those where players cooperate to optimize a common goal, while non-cooperative games are those where players don't cooperate. Furthermore, the use of a distributed architecture that incorporates prediction and detection algorithms allows for the optimisation of processes by using both mobile nodes and centralised infrastructure to enhance efficiency and effectiveness.

Game theory is commonly recognised as a mathematical framework that can be employed to analyze the dynamics of conflict between a defender (IDS) and attackers, with the aim of determining the optimal strategy for the defence in accurately identifying a suspicious target as malevolent [75]. Therefore, to safeguard the integrity of the prevailing intelligent network against significant and perhaps fatal cyber threats, a number of cyber games have been developed. These games predominantly employ non-cooperative game theory as a means to address issues pertaining to prediction and decision-making[76]. In the context of such a particular game, participants strive to optimise their own payoffs while simultaneously decreasing the payoffs of their adversaries.

The primary aim of a non-cooperative game is to establish a state of Nash Equilibrium (NE) between the attacker and the Intrusion Detection System (IDS)[77]. In this condition, the attacker deploys malicious software targeting networking and IoT nodes, while the IDS employs its detection mechanism to safeguard legitimate users. This article therefore proposes utilising the intruder attack pattern through channel modelling to facilitate the analysis of intrusions into host networks by employing game theory and devising counter-protection strategies.[78]. The security aspects of using different ML techniques in an adversarial system between intruders and authorised devices and users are also explored further in this article.

The game theory approach, which focuses on the interaction between users and attackers, along with its PD matrix, is briefly discussed.

Let us denote $\underset{User}{\text{Ű}}$ and $\underset{Attacker}{\text{Ű}}$ as the valid user and the intruder in the network. These players in the game possess a set of strategies $\mho_{user} = \{\phi_i^1 | i = 1,2,\ldots,m\}$ and $\mho_{attacker} = \{\phi_j^2 | j = 1,2,\ldots,n\}$, respectively, where m and n are the maximum number of strategies that the user and attacker can carry out respectively. Table VI depicts a multidimensional payoff matrix or the prisoner's dilemma (PD) matrix between these two players where a_{ji} and a'_{ji} are the rewards earned by $\underset{Attacker}{\text{Ű}}$ and $\underset{User}{\text{Ű}}$ respectively. The rewards earned by both players are defined by the strategies ϕ_i^1 and ϕ_j^2 performed in the given instances illustrated below:

Table 6. Multidimensional Payoff Reward Matrix.

Attacker Rewards (Host bandwidth access granted to the attacker)	$\underset{Attacker}{\text{Ű}}$ \ $\underset{User}{\text{Ű}}$	User Rewards (Host bandwidth access granted to the user)		
		ϕ_1^1	……	ϕ_m^1
	ϕ_1^2	(a_{11}, a'_{11})	…….	(a_{1m}, a'_{1m})
	…….	…….	…….	…….
	ϕ_n^2	(a_{n1}, a'_{n1})	…….	(a_{nm}, a'_{nm})

1. The rewards (a'_{ji}, a_{ji}) are earned by the players $\underset{User}{\text{Ű}}$ and $\underset{Attacker}{\text{Ű}}$ when IDS has not carried out the monitoring process yet the attacker has launched a malicious attack on the host network.
2. The rewards (a'_{ji}, a_{ji}) are earned by the players $\underset{User}{\text{Ű}}$ and $\underset{Attacker}{\text{Ű}}$ when IDS monitors the network while the attacker launches an attack on the host network.
3. The rewards (a'_{ji}, a_{ji}) are earned by the players $\underset{User}{\text{Ű}}$ and $\underset{Attacker}{\text{Ű}}$ when IDS runs a monitoring

 doi:10.20944/preprints202405.1066.v1

process and the attacker behaves like a normal node.

4. The rewards (a'_{ji}, a_{ji}) are earned by the players $\underset{User}{\text{Ű}}$ and $\underset{Attacker}{\text{Ű}}$ when IDS does not monitor the network and the attacker behaves like a normal node.

The matrix depicts the reward allocation for both the user and attacker in a game to gain access to the host bandwidth. The reward allocation under the applied game theory is done under various combinations of interactions between the user and the attacker and is categorised into four instances, as illustrated. The first instance takes place when the attacker has access to the host network and gains more rewards than the user when IDS fails to monitor the host network. The second instance illustrates the rewards earned by both attackers and users when IDS starts monitoring the host network immediately after the attacker launches its attack.

Furthermore, there can also be a scenario when an attacker behaves like a normal node after launching an attack, causing the host IDS to fail to detect its presence. Thus, rewards for this instance are allocated accordingly to the user and the attacker. The host network can thus, enhance its security by implementing effective countermeasures by thoroughly examining user and attacker situations. Pseudocode 1 effectively presents the attacking model, strategy setup, and protection mechanism for the proposed scenario using game theory, as illustrated in the flow process and shown in Figure 4.

The proposed intrusion detection scenario further aims to identify and combat security challenges in the IoT framework by focusing on perception, network, middleware, and application layers. It therefore suggests integrating network slicing, machine learning techniques, and a game theory approach to effectively address these challenges.

VI. Integration with Network Slicing and ML

The Internet of Things (IoT) has significant potential for the establishment of an intelligent society. Still, it faces various obstacles, such as developing networking and storage frameworks, efficient data communication protocols, implementing security measures, standardising technologies, managing devices and data, addressing diversity, and ensuring interoperability. Therefore, to address security challenges, it is crucial to improve and update host network security measures, including network slicing and training the concerned network, to meet specific requirements and address diverse security challenges.

Pseudocode 1: Attacking Model, Strategy Setup and Protection Mechanism for proposed system using Game Theory

Attack Model

Initialize the network:

Define Host network: (N); Intruders or compromised node: m; Valid users: $n = N - m$;

Resource Allocation: Assigning input parameters in the host network model:

Channel conditions: Rayleigh flat fading channel;

Channel gain: $10^{\left(\frac{-Path\ Loss}{10}\right)}$;

Power of the connecting base station: $\underset{BS}{\mathcal{P}}$;

Bandwidth assignment to connected nodes (whether an intruder or valid user) from equation (11) based on their SNR;

For $i = 1{:}N$

$Max\_BW = B_n^t$;

if $SNR_{user} > SNR_{attacker}$

Assign Max_BW to a valid user;

else

Assign Max_BW to the attacker;

end

end

 doi:10.20944/preprints202405.1066.v1

Strategy Setup: For Maximum BW Access

Initialize Payoff: using PD matrix (Table VI)

Obtain the SNR of the user and intruder from their path loss equations in different user scenarios;

From Step 2, compare SNRs for the user and the attacker:

If $SNR_{attacker} > SNR_{user}$

Maximum BW assigned to attacker;

end

Host BW is successfully accessed by an intruder.

Protection Mechanism

Initialize the active users: Valid user and intruder

Identify the connected users accessing host BW and create a datasheet;

Check user validity: from step 3;

If $n = valid\ user$

Assign BW (Step 2)

else if

If n= attacker

Generate alarm and remove node

else if n=compromised node

Remove node

end

end

Intruder or compromised node successfully removed and BW assigned to the user.

This paper thus, supports the use of network slicing and machine learning techniques in an intrusion detection system, utilizing game theory.

A. Network Slicing Integration with Proposed IDS

The network slicing of the IoT framework is usually incorporated into the network and middleware domains as per the proposed system, corroborating the security challenges in Figure 2. The concerned network can be sliced based on different user densities, including urban, outdoor, indoor, and remote areas, in terms of SNR, channel capacities, and throughputs, as illustrated in Figure 5, Figure 6 and Figure 7. Furthermore, the security of the network domain is crucial for all connecting devices, people, and cloud services, especially at network gateways.

Pseudocode2: Slicing the deployed network

Random node deployment:

No. of nodes to be deployed: n

No. of compromised nodes: m

No. of valid users: $n - m$

Set coordinates for x, y and z axis:

$x = \text{rand}(n, 1)$;

$y = \text{rand}(n, 1)$;

$z = \text{rand}(n, 1)$;

Create a 3D scatterplot: scatter3(x, y, z, n);

Define no. of slices:

no_slices = 5; (edge users, perception layer, network layer, middleware layer, application layer)

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2024 doi:10.20944/preprints202405.1066.v1

Slice range along the z-axis:

z_range = linspace(min(z), max(z), no_slices + 1);

Space between slices:

offset = (0,1];

Highlight the compromised nodes with '*'

z_range = z_range + offset;

Plot the sliced network

for i = 1: no_slices

idx = z ≥ z_range(i)& z < z_range(i + 1);

scatter3(x(idx), y(idx), z(idx));

end

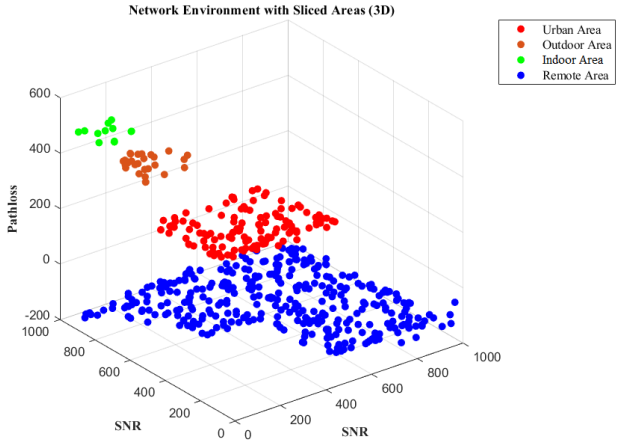

Figure 5. Network slicing of different user scenarios concerning their signal-to-noise ratios (SNRs).

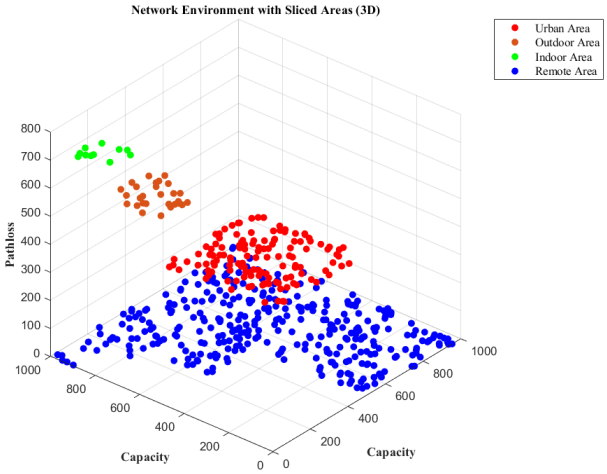

Figure 6. Network slicing of different user scenarios concerning their respective channel capacities.

 doi:10.20944/preprints202405.1066.v1

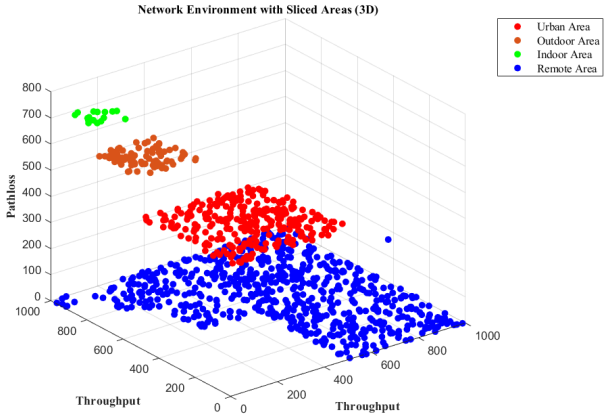

Figure 7. Network slicing of different user scenarios concerning their respective throughputs.

They offer hardware and software solutions for IoT devices, decrypt and encrypt IoT data, and translate between layers of communication protocols. IoT systems include LoraWAN, ZigBee, Z-wave, and TCP/IP platforms with multiple gateways [22].

IoT gateways face several security challenges, including secure onboarding, minimizing attack surface, end-to-end encryption, and firmware updates. Gateways, acting as intermediaries between devices and services, are vulnerable to man-in-the-middle attacks and eavesdropping, necessitating secure onboarding for encryption keys. Thus, to prevent such backdoor authentication and data breaches, IoT gateway manufacturers should only focus on designing essential interfaces and protocols and limit end-user services and functions. Furthermore, end-to-end encryption is necessary to ensure data confidentiality, but it is vulnerable to data breaches at the gateway level.

Recording firmware versions and verifying signature validity are essential for maintaining security in IoT gateways [12]. For the IoT framework being considered, pseudocode 2 helps set up the sliced network and identify the compromised nodes in the perception, network, middleware, and application layers. Here, the afore-discussed game theory may be applied to remove the access of such nodes to the host network. The simulated results demonstrate the use of network slicing in our scenario, highlighting machine learning techniques for intrusion detection in host networks and their integration with game theory mechanisms.

B. ML Integration with IoT

IoT has the potential to revolutionize various sectors like lifestyle, business, environment, and infrastructure due to its diverse devices, networks, and data types. Therefore, a scalable, adaptive, efficient, and fair management mechanism is needed for IoT networks [15]. Machine learning and deep learning further have the potential to revolutionize autonomous resource management and decision-making in large-scale, complex IoT systems, enabling real-time actions and adapting to environmental changes, contrasting the traditional methods like optimization and cooperative approaches. Network management however becomes challenging with large users or smart devices.

The research aims to integrate machine learning techniques into an intrusion detection system using game theory, demonstrating their implementation in a proposed system model. Some of the ML techniques to be used for detecting and classifying the intruder nodes from the valid users are discussed as follows:

1. Logistic Regression:

Logistic regression is a supervised machine learning technique that classifies dependent variables with independent ones, estimating the probability of a data point falling into a specific class based on input parameters. Hence, the multi-class logistic regression model, an extension of logistic regression over multiple features, uses the Softmax function to create a probability distribution for predicting the target class. This model can be applied to detect and predict intruders in a deployed network as per our scenario, as defined in (17).

 doi:10.20944/preprints202405.1066.v1

$$P(y = i, |x) = \frac{e^{w_i.x+b_i}}{\sum_{j=1}^{N} e^{w_j.x+b_j}} \quad (17)$$

Here P determines the probability of a connected node being an intruder. The weight vector 'w' represents the total connected entities, while 'b' is an adjustable bias term. The vector of variables 'x' comprises all the connected valid users, intruders, and compromised or failed nodes.

2. Bayesian Classifier:

Bayesian classifiers, based on the Bayes theorem, help predict class membership probabilities, ensuring that a data tuple X belongs to class C and can be used to classify intruder nodes accessing the host network. The Bayes theorem is the foundation for two classifiers: the Naïve Bayes classifier and Bayesian networks. Let X_{int} be a data tuple representing the evidence of an intruder, while H is some hypothesis representing the host network. According to Baye's theorem:

$$P(H|X_{int}) = \frac{P(X_{int}|H)P(H)}{P(X_{int})} \quad (18)$$

Where $P(H|X_{int})$is the probability that the hypothesis holds for the given evidence, in other words, the intruder's presence is confirmed by the host network. $P(H)$ is the prior probability of H, $P(X_{int}|H)$ is the posterior probability of X_{int} conditioned on H, while $P(X_{int})$ is the prior probability of X_{int}.

3. Support Vector Matrix (SVM):

Support Vector Machine (SVM) is a supervised learning technique used for classification and regression, plotting data in an N-dimensional space with N training features. It learns to predict and classify new incoming classes by training and testing network features with new data [79]. The mathematical equation for the support vector system is described in (19):

$$\sum_{i=1}^{n} \sum_{j=1}^{m} (wx) + b = 0 \quad (19)$$

Where x represents the input vector comprising of the connected n users and m intruders, w represents the weight vector distributed to the connected entities, and b is the bias term. These terms are learned during the model training phase to optimize a cost function, penalizing incorrect classifications and increasing the margin between target classes.

4. Decision Tree:

The decision tree is a machine learning algorithm utilized for regression and classification problems, maintaining a tree-like structure with specified features as nodes. The tree in the model represents the range of possible node values, including valid, intruder, and compromised nodes connected to the host network. It recursively creates branches while training, requiring the host network to check new data points and identify leaf nodes to determine the suspected node category [80]. Decision trees are adept at handling both categorical and continuous data, with leaf nodes determining the final predicted values from input parameters. Therefore, this approach can be applied to the proposed sliced network, with each model on an individual slice having varying decision nodes based on the host dataset's features.

5. K-Nearest Neighbour (KNN):

K-nearest neighbour (KNN) is a nonparametric supervised learning algorithm that classifies new data based on their closeness, enhancing model robustness without requiring prior knowledge about the data. The model determines if a network node is an intruder or a valid user by finding the k-closest points from a given data point and identifying the majority of connected classes, whether attackers or normal users. Hence, the most common value among the considered neighbours is predicted to be the target value for the suspected node. Therefore, in the case of intrusion detection, intruder elements are detected based on their nodal attribute analysis and accordingly assigned the cluster value [81].

6. K-Means Clustering:

It is an unsupervised learning technique that uses vectors as input to make inferences from data sets. It groups data into clusters with similar patterns and randomly selects K centroids. The

 doi:10.20944/preprints202405.1066.v1

algorithm works iteratively to assign each data point to the closest centroid using Euclidean distance, which finds similarities between data flows. The mean value of each data point is calculated for each centroid [82].

In the next section, we'll show the simulated results for the suggested system, which includes an intrusion detection system that uses game theory in different user-density scenarios. Intrusion detection is further used with a network-slicing approach in the IoT framework. The algorithms discussed above are also implied for the detection of suspected nodes in the host network.

VII. Simulation Results and Discussion

This section presents the simulation results of the suggested scenario using MATLAB and open-source Python. The system comprises a game-based intrusion detection system to be immersed with the host network, where the lost data is recovered through the channel capacities. The study analyzes and tabulates channel parameters like channel capacities, SNR, throughput, and efficiency for various user densities across rural, urban, suburban, and indoor network scenarios in Table VII, while Table VIII illustrates the simulation parameters used. The proposed scenario enables IoT networks to be sliced based on performance metrics like SNR, throughput, and channel capacity, considering different user scenarios and path loss models for urban, rural, outdoor, and indoor areas, as illustrated in Figures 5, 6, and 7.

Furthermore, game theory is hereby used to forecast future attacks in urban, remote, suburban, and indoor scenarios for 6G and IoT-based real-time applications. Results are simulated by applying the channel modelling approaches for different path loss models [83] shown in Figure 8 and Figure 9. Here the remote area has high coverage, while the urban area has a higher user density than the remote area, as shown by the comparative channel capacities before, during, and after the intrusion attacks in a host network. On the other hand, Figures 10 and 11 respectively depict intrusion detection and recovered capacity for suburban and indoor user density scenarios.

The suburban scenario coverage lies somewhere in between the urban and the indoor coverage user density, forming a neighbourhood area network(NaN). Therefore the NaN has less coverage but more user density than the urban coverage area due to the interconnectivity of the small cells and BSs with the user devices [84]. However, the indoor scenario has a higher user density but lesser coverage than NaN, urban and remote user coverage, due to high connectivity with IoT devices [85]. The graphs plotted and the comparative analysis in Table VIII reveal that the restored capacity for all user scenarios is slightly less than their original capacity.

This implies that data was lost during an attack on the host network. Likewise, the proposed intrusion detection scenario is further applied to the sliced IoT network, as previously discussed in Section III. The IoT framework slices, including the perception, network, middleware, and application layers, are highly susceptible to intrusion attacks, with the most prominent attacks depicted in Figure 2. The objective is to effectively separate intruders or compromised nodes from valid users in each IoT layer, thereby harmonizing network slicing.

Figures 13 and 14 thus help illustrate and compare the proposed scenarios of intrusion detection without and with slicing, respectively. The proposed scenario further utilises machine learning techniques such as SVM, KNN, decision trees, and K means to categorise complex networks, identify suspicious elements, and distinguish invalid users from legitimate ones after using the game theory, as described earlier. The support vector machine (SVM) classification model here aims to identify a hyperplane that divides network nodes into target classes like intruders and valid users, creating a decision boundary, while the non-linear classification model uses a kernel function to map data to an N-dimensional space. The SVM classifier here divides data into groups using a hyperplane, classifying new data into target classes based on the positive or negative sign as shown in Figure 12.

The decision tree in the proposed system model checks if a given data point is an intruder, compromised node, or valid user. It then moves to the next decision node, checking the value for another feature, and ends at the leaf node, determining the node status value, and helping distinguish between intruders and valid users, as illustrated in Figure 15. Here, Gini impurity, also known as the Gini index, is a measure of data disorder in decision trees used to split nodes during training,

 doi:10.20944/preprints202405.1066.v1

indicating the degree of data impurity. This is calculated for a binary classification problem involving two classes (valid user and

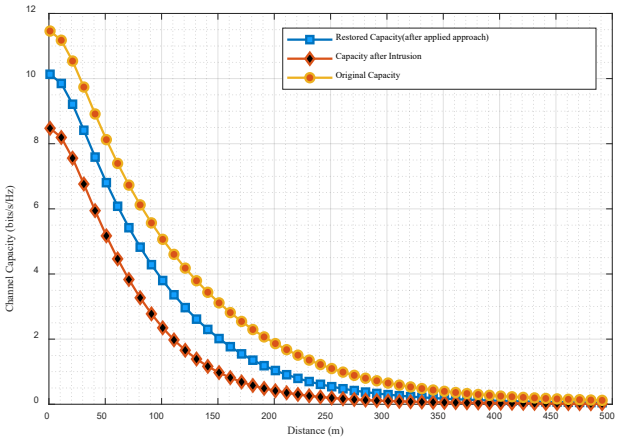

Figure 8. Intrusion detection from bandwidth spoofing and improved channel capacity from intrusion in network deployed in a remote user scenario.

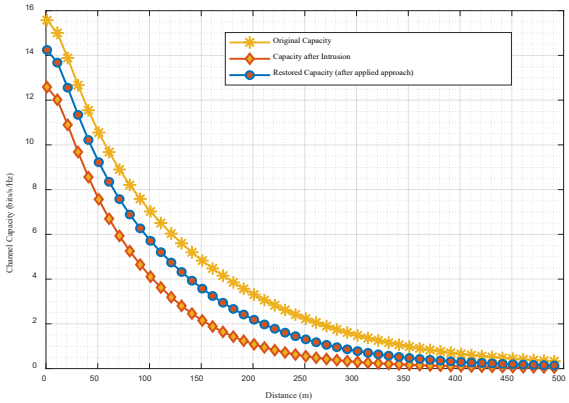

Figure 9. Intrusion detection from bandwidth spoofing and improved channel capacity from intrusion in network deployed in an urban user scenario.

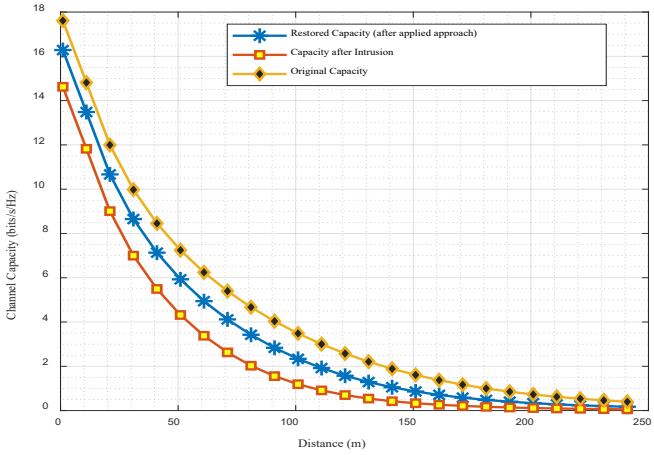

Figure 10. Intrusion detection from bandwidth spoofing and improved channel capacity from intrusion in network deployed in a suburban scenario with intermediate user density.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2024 doi:10.20944/preprints202405.1066.v1

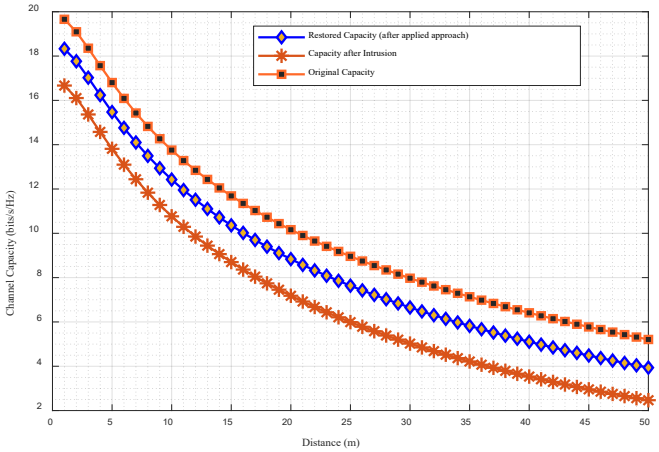

Figure 11. Intrusion detection from bandwidth spoofing and improved channel capacity from intrusion in network deployed in an indoor user scenario with high user connectivity.

TABLE 7. Simulation Parameters.

Parameter	Value
Frequency(f)	28 GHz
Bandwidth	800 MHz
Noise figure	-106dBm
Maximum coverage d	500m
Maximum transmission power	30dBm
Minimum transmission power	18dBm
Pathloss exponent (α)	2 to 4
Pathloss of a neighbourhood area network	$13.54 + 20log_{10}(f) + 39.08log_{10}(d)\ dB$
Pathloss of the urban user area	$28.0 + 20log_{10}(f) + 40log_{10}(d) - 24.6792\ dB$
Pathloss of indoor area network	$17.30 + 24.9log_{10}(f) + 38.3log_{10}(d)dB$
Path loss of remote user area	$148.1 + 37.6log_{10}(d)\ dB$
Channel gain formula for a given path loss	$10^{(\frac{-Path\ Loss}{10})}$

intruder or compromised node), in our context, using the following formula:

$$Gini\ impurity = 1 - \sum_{i=1}^{k} p_i^2 \quad (20)$$

where k is the number of classes, and p_i is the probability of belonging to class i. Gini impurity is used to measure class separation in decision trees. It determines the best split at each node during training, as lower Gini values indicate more homogeneous nodes. The Gini index, therefore, represents the impurity at each decision point in a decision tree plot.

Furthermore, the KNN algorithm is a lazy learning method that predicts values from training data and stores them in its memory space. It uses the Euclidean distance metric to check the nearest points to a node's validity, considering $k = 5$ nearest points in our context. The algorithm uses this data to determine the status of the new data point, whether it is an intruder or a valid user. The majority of these points are chosen as the predicted status for the new data point, as shown in Figure 16. The K-means clustering algorithm, on the other hand, is a method used to group data into clusters with similar patterns, randomly selecting K centroids using Euclidean distance and separating intruder nodes from valid users by identifying similarities between data flows, as shown in Figure 17.

Table IX presents the hyperparameters utilized in executing the aforementioned algorithms following our specific scenario. As discussed previously, the flow process for our proposed system illustrates the use of the host network database to check the presence of intruders. Therefore, we make use of some of the machine-learning classification techniques discussed previously to predict

 doi:10.20944/preprints202405.1066.v1

and detect the intruder's presence in the given host network, where the intruder is most likely to behave as a normal user to gain access to the host bandwidth.

Table 8. Comparative Analysis of Channel Parameters Before, During and After the Host Network Intrusion.

	Parameters	Before Intrusion			During Intrusion			After Intrusion		
		SNR	Channel Capacity (bits/s/Hz)	Throughput (bps)	SNR	Channel Capacity (bits/s/Hz)	Throughput (bps)	SNR	Channel Capacity (bits/s/Hz)	Throughput (bps)
User Scenarios	Urban user coverage (d=500m)	0.23	0.3075	246020000	0.029	0.042	34014000	0.09	0.1304	104300000
	Remote user coverage (d=500m)	0.51	0.59	479230000	0.06	0.09	72463000	0.20	0.26	215140000
	Urban micro: Neighbourhood area network (NaN)(d=250m)	0.27	0.35	280100000	0.034	0.049	39235000	0.10	0.149	119770000
	Indoor Scenario (d=50m)	35.92	5.20	4165400000	4.52	2.46	1972400000	14.30	3.93	3148700000

Table 9. Hyperparameters for Applied ML Algorithms.

Description	Value
Frequency	28GHz
Bandwidth	800MHz
No. of nodes deployed (N)	10 to 50
No. of intruder nodes considered (I)	$1/5(N)$
No. of failed or compromised nodes (F)	$1/10(N)$
No. of valid users (U)	$N-(I+F)$

A. Future Challenges and Research Aspects

To protect user applications from imploding, AI and ML models, along with robust authentication, are necessary, requiring trust mechanisms for proper operations in virtual network functions in the host network. Therefore the open radio access network (ORAN) architecture integrates security functions into containerized virtual network functions (VNFs), enabling the prevention, detection, and mitigation of attacks through traffic monitoring, enabling fast on-demand service deployment, surpassing the capabilities of 5G and 6G systems [86]. The system provides virtualization, intelligence, and flexibility, in addition to establishing open interfaces to facilitate network innovation. ORAN leverages the use of SDN and network function virtualization (NFV) technologies to disassemble conventional RAN functions and interconnect them via standardised interfaces [87].

Third-party cloud platforms are shared among telecommunication operators, therefore, posing risks of insider attacks. ORAN provides a storage facility for data plane flow behaviour and flow statistics, enabling SDN controllers to retrieve these without increasing overhead [88]. This ensures the consistent implementation of security policies and dynamic protection of AI controllers. The integration of AI and ML methodologies warrants careful consideration for the enhancement of wireless network security mechanisms, including crucial aspects such as authentication, authorization, encryption, and validation [89].

Physical layer security attacks often mislead AI models and disrupt wireless communication performance. Therefore, to mitigate these attacks and ensure the robustness of AI models, adversarial training is a common defence mechanism [86]. The process involves repeatedly using adversarial

 doi:10.20944/preprints202405.1066.v1

samples and retraining a host network model with positive samples and labels to create a sophisticated, well-trained host network that prevents hackers from altering their configurations and can be retrained once the attacker identifies the configuration. The 6G blockchain offers a decentralised and secure communication infrastructure that facilitates network virtualization and slicing.

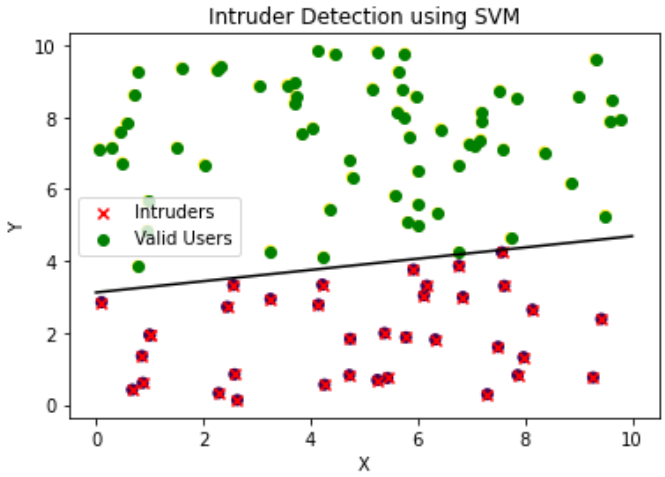

Figure 12. Intruder nodes detection and separation from valid users in a host network using support vector machine (SVM) algorithm.

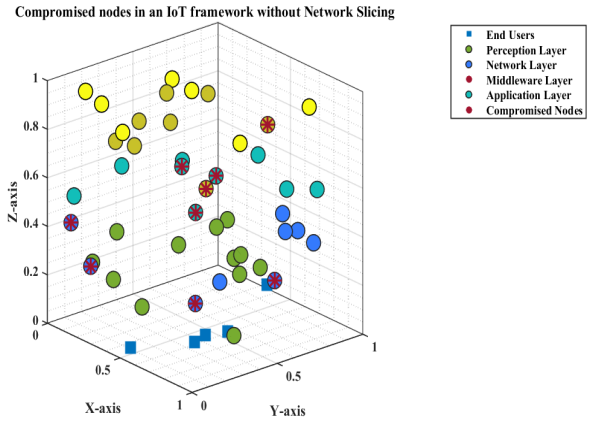

Figure 13. Intruder node presence with other users and edge devices in an unsliced IoT framework.

This architecture enables the implementation of smart contracts, which may be used for slice trade and the management of service-level agreements (SLAs). The integrated blockchain records resource usage and service provider performance, while the distributed ledger ensures data integrity against tampering. This integration also provides a storage scheme for training data [90]. 6G systems require system integrity and security to adapt to hardware and software changes, with wireless network security being a key feature. Therefore, research is crucial in this aspect to minimise network vulnerabilities and safeguard advanced use cases, enhancing wireless network security in 6G and IoT systems.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 May 2024 doi:10.20944/preprints202405.1066.v1

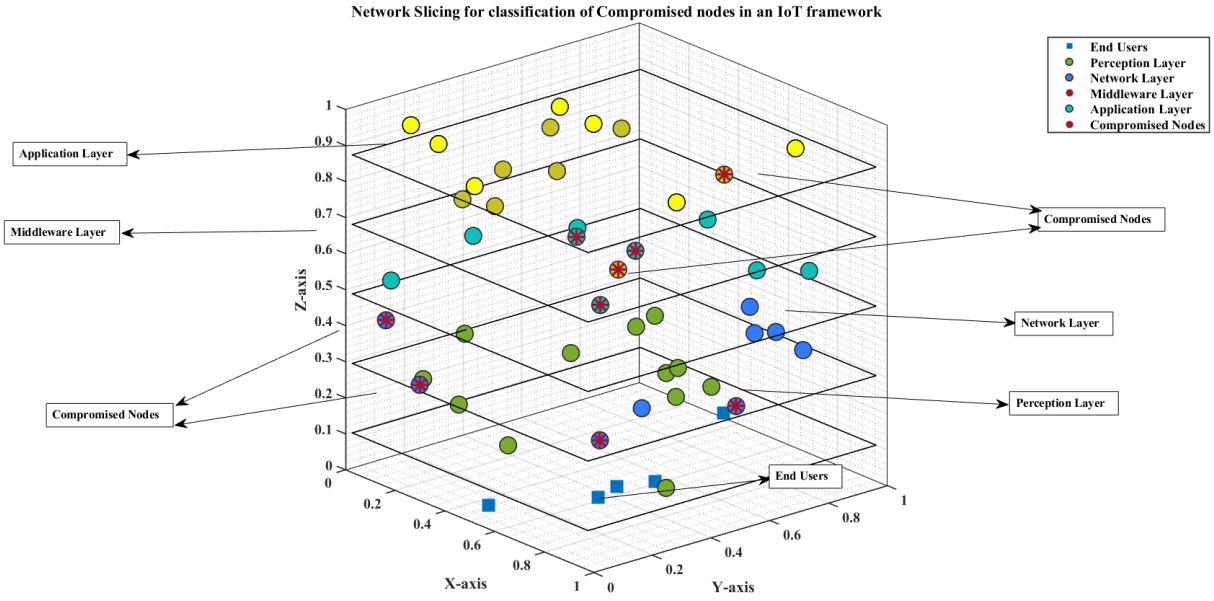

Figure 14. Effective detection and segregation of the intruder nodes from the rest of the connected devices in a sliced-layered IoT framework.

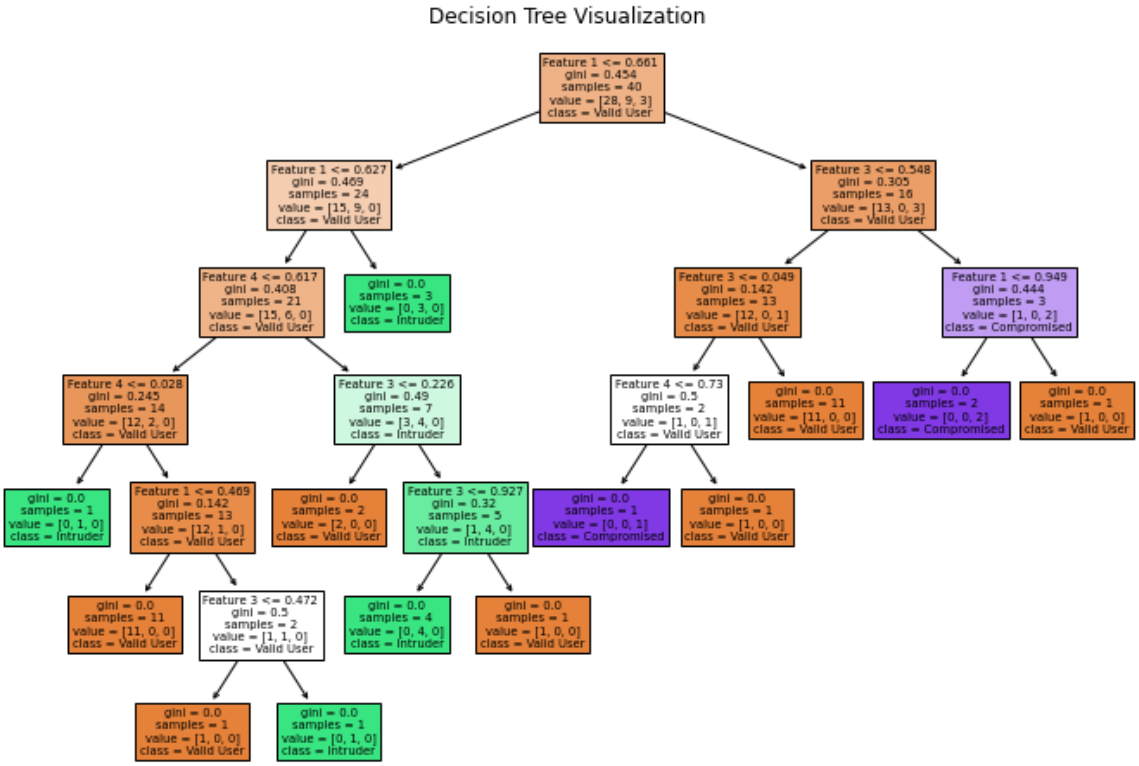

Figure 15. Intruder nodes segregation from valid users in a host network using decision tree algorithm.

VIII. Conclusion

The security of wireless communication networks supporting B5G and 6G is a top priority due to increasing cyberattacks and complex behaviours, with 6G networks expected to enhance mobile

 doi:10.20944/preprints202405.1066.v1

broadband and IoT coverage. Since the emergence of IoT and IoE, data security has been a major concern, impacting host systems. The security of the existing wireless networks is crucial, and updating the security system is necessary to prepare for future intrusions. However, it is not possible to completely remove all intrusive features at once, so communication systems must be modified to prepare for future intrusion attacks.

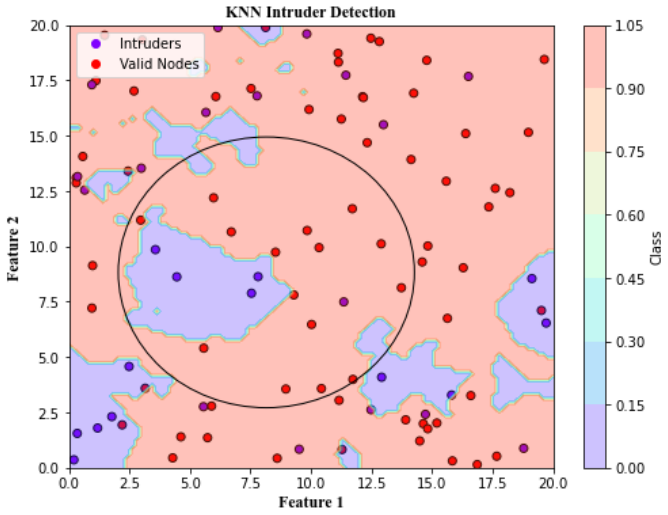

Figure 16. Intruder nodes segregation from valid users in a host network using the K-Nearest Neighbour(KNN) algorithm.

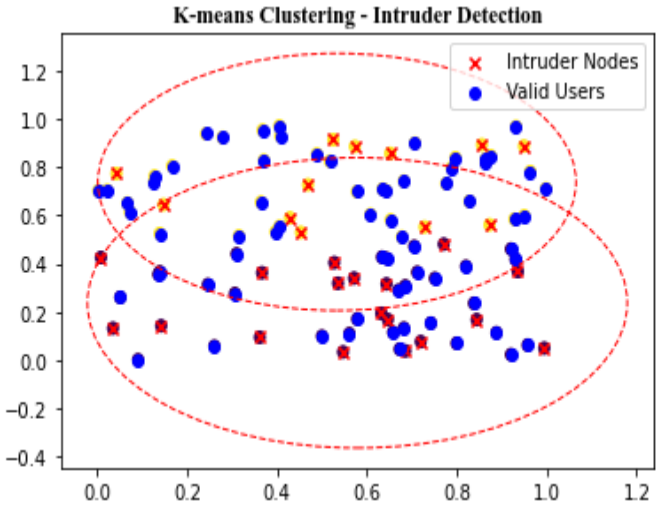

Figure 17. Intruder nodes segregation from valid users in a host network using the K-Means Clustering algorithm.

The use of AI and ML algorithms can thus improve wireless network security by enhancing attack patterns and improving discovery and recovery capabilities. On the other hand, attackers can use network faults using game theory to learn more about user data, how networks work, and how systems are managed, as discussed in previous sections, which lets them come up with more advanced attack plans. Furthermore, the system proposes network slicing to detect such attacks across all layers of the IoT framework.

The article also discusses machine learning techniques for classifying and segregating attacker elements from normal users in host networks, offering applications in long-distance and high-mobility communications with low power consumption. However, AI/ML models can be compromised through various attack vectors like data extraction, model information extraction, and

misinterpretation, using active or passive methods to alter the original host dataset. Thus, the future host network should be trained and updated using AI and ML techniques inside the layered 6G networks.

Acknowledgement: The Authors Gratefully Acknowledge The Support Provided By 5g And Iot Lab, Soece, Smvdu, And Central University Jammu.

References

1. G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, '6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence', *IEEE Wirel. Commun.*, vol. 27, no. 5, pp. 126–132, 2020, doi: 10.1109/MWC.001.1900516.
2. M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, 'Edge and fog computing for IoT: A survey on current research activities & future directions', *Comput. Commun.*, vol. 180, pp. 210–231, 2021, doi: https://doi.org/10.1016/j.comcom.2021.09.003.
3. Z. Zhang *et al.*, '6G wireless networks: Vision, requirements, architecture, and key technologies', *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, 2019.
4. K. David and H. Berndt, '6G vision and requirements: Is there any need for beyond 5G?', *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, 2018.
5. C. D. Alwis *et al.*, 'Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research', *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021, doi: 10.1109/OJCOMS.2021.3071496.
6. G. Geraci *et al.*, 'What Will the Future of UAV Cellular Communications Be? A Flight From 5G to 6G', *IEEE Commun. Surv. Tutor.*, vol. 24, no. 3, pp. 1304–1335, 2022, doi: 10.1109/COMST.2022.3171135.
7. A. E. Omolara *et al.*, 'The internet of things security: A survey encompassing unexplored areas and new insights', *Comput. Secur.*, vol. 112, p. 102494, 2022, doi: https://doi.org/10.1016/j.cose.2021.102494.
8. S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, 'What should 6G be?', *Nat. Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020, doi: 10.1038/s41928-019-0355-6.
9. F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, 'Enabling Massive IoT Toward 6G: A Comprehensive Survey', *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891–11915, Aug. 2021, doi: 10.1109/JIOT.2021.3063686.
10. D. C. Nguyen *et al.*, '6G Internet of Things: A Comprehensive Survey', *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022, doi: 10.1109/JIOT.2021.3103320.
11. M. Vaezi *et al.*, 'Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Toward 6G', *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 1117–1174, 2022, doi: 10.1109/COMST.2022.3151028.
12. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, 'A survey on IoT security: application areas, security threats, and solution architectures', *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
13. A. Aijaz, 'Hap-SliceR : A Radio Resource Slicing Framework for 5G Networks With Haptic Communications', *IEEE Syst. J.*, vol. 12, no. 3, pp. 2285–2296, Sep. 2018.
14. M. Yan, G. Feng, J. Zhou, Y. Sun, and Y.-C. Liang, 'Intelligent Resource Scheduling for 5G Radio Access Network Slicing', *IEEE Trans Veh Technol*, vol. 68, no. 8, pp. 7691–7703, 2019, doi: 10.1109/tvt.2019.2922668.
15. F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, 'Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges', *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1251–1275, 2020, doi: 10.1109/COMST.2020.2964534.
16. M. Alsenwi, N. H. Tran, M. Bennis, S. R. Pandey, A. K. Bairagi, and C. S. Hong, 'Intelligent Resource Slicing for eMBB and URLLC Coexistence in 5G and Beyond: A Deep Reinforcement Learning Based Approach', *IEEE Trans. Wirel. Commun.*, vol. 20, no. 7, pp. 4585–4600, 2021, doi: 10.1109/TWC.2021.3060514.
17. K. Zhang, Z. Yang, and T. Başar, 'Multi-Agent Reinforcement Learning: A Selective Overview of Theories and Algorithms', in *Handbook of Reinforcement Learning and Control*, K. G. Vamvoudakis, Y. Wan, F. L. Lewis, and D. Cansever, Eds., Cham: Springer International Publishing, 2021, pp. 321–384. doi: 10.1007/978-3-030-60990-0_12.
18. A. K. Kamboj, P. Jindal, and P. Verma, 'Machine learning-based physical layer security: techniques, open challenges, and applications', *Wirel. Netw.*, vol. 27, no. 8, pp. 5351–5383, Nov. 2021, doi: 10.1007/s11276-021-02781-1.
19. Y. Xu, Y. Wang, J. Ma, and Q. Jin, 'PSARE: A RL-Based Online Participant Selection Scheme Incorporating Area Coverage Ratio and Degree in Mobile Crowdsensing', *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 10923–10933, Oct. 2022, doi: 10.1109/TVT.2022.3183607.
20. B. Mughal, Z. Md. Fadlullah, M. M. Fouda, and S. Ikki, 'Optimizing Packet Forwarding Performance in Multiband Relay Networks via Customized Reinforcement Learning', *IEEE Open J. Commun. Soc.*, vol. 3, pp. 973–985, 2022, doi: 10.1109/OJCOMS.2022.3183172.

21. Y. Wang *et al.*, 'Adversarial Attacks and Defenses in Machine Learning-Empowered Communication Systems and Networks: A Contemporary Survey', *IEEE Commun. Surv. Tutor.*, pp. 1–1, 2023, doi: 10.1109/COMST.2023.3319492.
22. M. Gupta, R. K. Jha, and S. Jain, 'Tactile Based Intelligence Touch Technology in IoT Configured WCN in B5G/6G-A Survey', *IEEE Access*, vol. 11, pp. 30639–30689, 2023, doi: 10.1109/ACCESS.2022.3148473.
23. A. Gupta, R. K. Jha, P. Gandotra, and S. Jain, 'Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network', *IEEE Trans Veh Technol*, 2018, doi: 10.1109/TVT.2017.2745110.
24. P. Srividya, L. N. Devi, and A. N. Rao, 'A trusted effective approach for forecasting the failure of data link and intrusion in wireless sensor networks', *Theor. Comput. Sci.*, vol. 941, pp. 1–13, 2023, doi: https://doi.org/10.1016/j.tcs.2022.08.004.
25. V. Fanibhare, N. I. Sarkar, and A. Al-Anbuky, 'A Survey of the Tactile Internet: Design Issues and Challenges, Applications, and Future Directions', *Electronics*, vol. 10, no. 17, 2021, doi: 10.3390/electronics10172171.
26. R. N. N and H. V. Nath, 'Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges', *Comput. Electr. Eng.*, vol. 100, p. 107997, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107997.
27. I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and J. J. Rodrigues, 'Tactile internet for smart communities in 5g: An insight for noma-based solutions', *IEEE Trans. Ind. Inform.*, vol. 15, no. 5, pp. 3104–3112, 2019.
28. H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, 'Blockchain-enabled resource management and sharing for 6G communications', *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 261–269, 2020.
29. A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, 'A Survey of Security in Cloud, Edge, and Fog Computing', *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030927.
30. K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, 'SDN-Enabled Secure IoT Architecture', *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6549–6564, 2020.
31. S. Shahzadi *et al.*, 'Machine Learning Empowered Security Management and Quality of Service Provision in SDN-NFV Environment', *CMC-Comput. Mater. Contin.*, vol. 66, no. 3, pp. 2723–2749, 2021.
32. S. M. Aldossari and K.-C. Chen, 'Machine learning for wireless communication channel modeling: An overview', *Wirel. Pers. Commun.*, vol. 106, no. 1, pp. 41–70, 2019.
33. C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, 'Machine Learning Paradigms for Next-Generation Wireless Networks', *IEEE Wirel. Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017, doi: 10.1109/MWC.2016.1500356WC.
34. A. Chen, Y. Fu, X. Zheng, and G. Lu, 'An efficient network behavior anomaly detection using a hybrid DBN-LSTM network', *Comput. Secur.*, vol. 114, p. 102600, 2022, doi: https://doi.org/10.1016/j.cose.2021.102600.
35. T. E. Bogale, X. Wang, and L. B. Le, 'Machine Intelligence Techniques for Next-Generation Context-Aware Wireless Networks', *ITU Spec. Issue Impact Artif. Intell. AI Commun. Netw. Serv.*, 2018, doi: https://doi.org/10.48550/arXiv.1801.04223.
36. D. Gündüz, P. de Kerret, N. D. Sidiropoulos, D. Gesbert, C. R. Murthy, and M. van der Schaar, 'Machine Learning in the Air', *IEEE J. Sel. Areas Commun.*, vol. 37, no. 10, pp. 2184–2199, Oct. 2019, doi: 10.1109/JSAC.2019.2933969.
37. M. A. da Cruz, J. J. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi, and V. Korotaev, 'Performance evaluation of IoT middleware', *J. Netw. Comput. Appl.*, vol. 109, pp. 53–65, 2018.
38. B. Alzahrani, O. S. Oubbati, A. Barnawi, M. Atiquzzaman, and D. Alghazzawi, 'UAV assistance paradigm: State-of-the-art in applications and challenges', *J. Netw. Comput. Appl.*, vol. 166, p. 102706, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102706.
39. T. Taleb, S. Dutta, A. Ksentini, M. Iqbal, and H. Flinck, 'Mobile Edge Computing Potential in Making Cities Smarter', *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 38–43, Mar. 2017, doi: 10.1109/MCOM.2017.1600249CM.
40. Y. Xiao, G. Shi, Y. Li, W. Saad, and H. V. Poor, 'Toward self-learning edge intelligence in 6G', *IEEE Commun. Mag.*, vol. 58, no. 12, pp. 34–40, 2020.
41. D. Fudenberg and J. Tirole, 'Game theory, The MIT Press', *Camb. MA*, vol. 86, 1991.
42. M. Samir, D. Ebrahimi, C. Assi, S. Sharafeddine, and A. Ghrayeb, 'Leveraging Uavs for Coverage in Cell-Free Vehicular Networks: A Deep Reinforcement Learning Approach', *IEEE Trans. Mob. Comput.*, vol. 20, no. 09, pp. 2835–2847, Sep. 2021, doi: 10.1109/TMC.2020.2991326.
43. S. Bi, R. Zhang, Z. Ding, and S. Cui, 'Wireless communications in the era of big data', *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 190–199, 2015.
44. A. Alnoman, S. K. Sharma, W. Ejaz, and A. Anpalagan, 'Emerging edge computing technologies for distributed IoT systems', *IEEE Netw.*, vol. 33, no. 6, pp. 140–147, 2019.
45. I. Afolabi, A. Ksentini, M. Bagaa, T. Taleb, M. Corici, and A. Nakao, 'Towards 5G network slicing over multiple-domains', *IEICE Trans. Commun.*, vol. 100, no. 11, pp. 1992–2006, 2017, doi: 10.1587/transcom.2016NNI0002.

46. L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, '6G Wireless Systems: A Vision, Architectural Elements, and Future Directions', *IEEE Access*, vol. 8, pp. 147029–147044, 2020, doi: 10.1109/ACCESS.2020.3015289.
47. A. Al-Dulaimi, X. Wang, and I. Chih-Lin, *5G networks: fundamental requirements, enabling technologies, and operations management*. John Wiley & Sons, 2018.
48. J. Liu *et al.*, 'Initial Access, Mobility, and User-Centric Multi-Beam Operation in 5G New Radio', *IEEE Commun Mag*, vol. 56, no. 3, pp. 35–41, 2018, doi: 10.1109/MCOM.2018.1700827.
49. F. Al-Turjman, E. Ever, and H. Zahmatkesh, 'Small Cells in the Forthcoming 5G/IoT: Traffic Modelling and Deployment Overview', *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 28–65, 2019, doi: 10.1109/COMST.2018.2864779.
50. B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, '6G Technologies: Key Drivers, Core Requirements, System Architectures, and Enabling Technologies', *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 18–27, 2019, doi: 10.1109/MVT.2019.2921398.
51. J. Choi, 'On Delay-Constrained Transmissions of a Finite Number of Short-Length Packets', *IEEE Access*, vol. 9, pp. 1005–1015, 2021, doi: 10.1109/ACCESS.2020.3047092.
52. M. Gupta, R. K. Jha, and M. Sabraj, 'Touch-Interfacing Middleware Network Design in 6G', in *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Jan. 2023, pp. 345–349. doi: 10.1109/COMSNETS56262.2023.10041291.
53. S. Akbar, Y. Deng, A. Nallanathan, M. Elkashlan, and G. K. Karagiannidis, 'Massive multiuser MIMO in heterogeneous cellular networks with full duplex small cells', *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4704–4719, 2017.
54. Y. Yuan *et al.*, 'A 3D Geometry-Based Reconfigurable Intelligent Surfaces-Assisted MmWave Channel Model for High-Speed Train Communications', *IEEE Trans. Veh. Technol.*, pp. 1–16, 2023, doi: 10.1109/TVT.2023.3321645.
55. S. S. Omar, A. M. A. El-Haleem, I. I. Ibrahim, and A. M. Saleh, 'Capacity Enhancement of Flying-IRS Assisted 6G THz Network Using Deep Reinforcement Learning', *IEEE Access*, vol. 11, pp. 101616–101629, 2023, doi: 10.1109/ACCESS.2023.3315660.
56. C. Su, J. Zhang, and Y. Ji, 'Cyclic transmission window-based bandwidth allocation scheme for asynchronous time-sensitive industrial applications in TDM-PON', *J Opt Commun Netw*, vol. 15, no. 11, pp. 820–829, Nov. 2023, doi: 10.1364/JOCN.497848.
57. A. Ali and W. Hamouda, 'Advances on Spectrum Sensing for Cognitive Radio Networks: Theory and Applications', *IEEE Commun. Surv. Tutor.*, vol. 19, no. 2, pp. 1277–1304, 2017, doi: 10.1109/COMST.2016.2631080.
58. T. Ji, M. Hua, C. Li, Y. Huang, and L. Yang, 'Exploiting Intelligent Reflecting Surface for Enhancing Full-Duplex Wireless-Powered Communication Networks', *IEEE Trans. Commun.*, pp. 1–1, 2023, doi: 10.1109/TCOMM.2023.3323532.
59. A. Mabrouk and R. Zayani, 'Toward Energy-Efficient 6G Networks: Uplink Cell-Free Massive MIMO With NLD Cancellation Technique of Hardware Impairments', *IEEE Access*, vol. 11, pp. 105314–105329, 2023, doi: 10.1109/ACCESS.2023.3318882.
60. S. Mukherjee, C. Beard, and S. Song, 'Transformers for Green Semantic Communication: Less Energy, More Semantics'. 2023.
61. C. Zheng, F.-C. Zheng, J. Luo, P. Zhu, X. You, and D. Feng, 'Differential Modulation for Short Packet Transmission in URLLC'. 2023.
62. S. Weithoffer, G. Aousaji, J. Nadal, and C. A. Nour, 'Iteration Overlap for Low-Latency Turbo Decoding', in *2023 12th International Symposium on Topics in Coding (ISTC)*, Sep. 2023, pp. 1–5. doi: 10.1109/ISTC57237.2023.10273532.
63. W. Nie, M. Liu, J. Chen, W. Tan, and C. Li, 'Spectrum and Energy Efficiency of Massive MIMO for Hybrid Architectures With Phase Shifter and Switches in IoT Networks', *IEEE Internet Things J.*, pp. 1–1, 2023, doi: 10.1109/JIOT.2023.3323471.
64. D. Malak, F. V. Mutlu, J. Zhang, and E. M. Yeh, 'Joint Power Control and Caching for Transmission Delay Minimization in Wireless HetNets', *IEEEACM Trans. Netw.*, pp. 1–16, 2023, doi: 10.1109/TNET.2023.3319674.
65. A. Al-Dweik, E. Alsusa, O. A. Dobre, and R. Hamila, 'Multi-Symbol Rate NOMA for Improving Connectivity in 6G Communications Networks', *IEEE Commun. Mag.*, pp. 1–7, 2023, doi: 10.1109/MCOM.001.2300351.
66. J. C. M. Filho, T. Abrao, E. Hossain, and A. Mezghani, 'Reconfigurable Intelligent Surfaces-Enabled Intra-Cell Pilot Reuse in Massive MIMO Systems'. 2023.
67. H. Wang, Y. Bai, and X. Xie, 'Deep Reinforcement Learning Based Resource Allocation in Delay-Tolerance-Aware 5G Industrial IoT Systems', *IEEE Trans. Commun.*, pp. 1–1, 2023, doi: 10.1109/TCOMM.2023.3322736.

68. B. Guo, Y. Chen, P. Cheng, M. Ding, J. Hu, and L. Hanzo, 'Pareto-Optimal Multi-Agent Cooperative Caching Relying on Multi-Policy Reinforcement Learning', *IEEE Internet Things J.*, pp. 1–1, 2023, doi: 10.1109/JIOT.2023.3317971.
69. R. Carmona and F. Delarue, *Probabilistic Theory of Mean Field Games with Applications II: Mean Field Games with Common Noise and Master Equations*, vol. 84. Springer, 2018.
70. C.-X. Wang, J. Huang, H. Wang, X. Gao, X. You, and Y. Hao, '6G Wireless Channel Measurements and Models: Trends and Challenges', *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 22–32, 2020, doi: 10.1109/MVT.2020.3018436.
71. H. Sedjelmaci, S. M. Senouci, and N. Ansari, 'Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology', *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 5, pp. 1143–1153, 2017, doi: 10.1109/TITS.2016.2600370.
72. S. Sharma and A. Kaul, 'VANETs Cloud: Architecture, Applications, Challenges, and Issues', *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 2081–2102, 2021, doi: 10.1007/s11831-020-09447-9.
73. H. Liu, L. Yang, and H. Yang, 'Cooperative Optimal Control of the Following Operation of High-Speed Trains', *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 17744–17755, Oct. 2022, doi: 10.1109/TITS.2022.3163971.
74. V. Kumar and D. Sinha, 'A robust intelligent zero-day cyber-attack detection technique', *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2211–2234, Oct. 2021, doi: 10.1007/s40747-021-00396-9.
75. H. Sedjelmaci, M. Hadji, and N. Ansari, 'Cyber security game for intelligent transportation systems', *IEEE Netw.*, vol. 33, no. 4, pp. 216–222, 2019.
76. H. Sedjelmaci, S. M. Senouci, and N. Ansari, 'A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks', *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 48, no. 9, pp. 1594–1606, 2018.
77. K. Lu, G. Jing, and L. Wang, 'Distributed algorithms for searching generalized Nash equilibrium of noncooperative games', *IEEE Trans. Cybern.*, vol. 49, no. 6, pp. 2362–2371, 2018.
78. A. Gupta, R. K. Jha, and S. Jain, 'Attack modeling and intrusion detection system for 5G wireless communication network', *Int. J. Commun. Syst.*, vol. 30, no. 10, p. e3237, 2017.
79. A. Charrada and A. Samet, 'Joint interpolation for LTE downlink channel estimation in very high-mobility environments with support vector machine regression', *IET Commun.*, vol. 10, no. 17, pp. 2435–2444, 2016.
80. A. P. Kulkarni, N. Saxena, and A. Roy, 'Efficient Video QoE Prediction in Intelligent O-RAN.', *Comput. Netw. Commun.*, vol. 1, no. 2, pp. 343–356, 2023, doi: https://doi.org/10.37256/cnc.1220233661.
81. S. Zhang, X. Li, M. Zong, X. Zhu, and D. Cheng, 'Learning k for KNN Classification', *ACM Trans Intell Syst Technol*, vol. 8, no. 3, Jan. 2017, doi: 10.1145/2990508.
82. U. Challita, A. Ferdowsi, M. Chen, and W. Saad, 'Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs', *IEEE Wirel. Commun.*, vol. 26, no. 1, pp. 28–35, 2019, doi: 10.1109/MWC.2018.1800155.
83. D. G. Riviello, F. Di Stasio, and R. Tuninato, 'Performance Analysis of Multi-User MIMO Schemes under Realistic 3GPP 3-D Channel Model for 5G mmWave Cellular Networks', *Electronics*, vol. 11, no. 3, 2022, doi: 10.3390/electronics11030330.
84. S. Khan, 'The 5G Network Backbone: A Guide to Small Cell Technology', Telit. Accessed: Feb. 06, 2024. [Online]. Available: https://www.telit.com/blog/5g-networks-guide-to-small-cell-technology/
85. M. Dangana, S. Ansari, Q. H. Abbasi, S. Hussain, and M. A. Imran, 'Suitability of NB-IoT for Indoor Industrial Environment: A Survey and Insights.', *Sensors*, vol. 21, no. 16, Aug. 2021, doi: 10.3390/s21165284.
86. T. F. Rahman, A. S. Abdalla, K. Powell, W. AlQwider, and V. Marojevic, 'Network and Physical Layer Attacks and countermeasures to AI-Enabled 6G O-RAN'. 2022.
87. A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, '5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges', *Comput. Netw.*, vol. 167, p. 106984, 2020.
88. S. Sharma, R. Miller, and A. Francini, 'A cloud-native approach to 5G network slicing', *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 120–127, 2017.
89. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, 'A survey of machine and deep learning methods for internet of things (IoT) security', *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1646–1685, 2020.
90. K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, 'Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G', *IET Commun.*, vol. 12, no. 5, pp. 527–532, 2018

 doi:10.20944/preprints202405.1066.v1

MANTISHA GUPTA (Student Member, IEEE) received her B.E degree in Electronics and Communication Engineering from Jammu University, J&K, India in 2017 and the M.Tech Degree in Electronics and Communication Engineering from Shri Mata Vaishno Devi University(SMVDU), Katra, Jammu, J&K, India in 2019. She is pursuing a PhD in IoT-configured networks in B5G/6G wireless communication systems from the School of Electronics and Communication Engineering(SoECE), at Shri Mata Vaishno Devi University (SMVDU). She is a student member of the Institute of Electrical and Electronics Engineers (IEEE).

RAKESH KUMAR JHA (Senior Member, IEEE) received the B.Tech. degree (Hons.) in electronics and communication engineering, the M.Tech. degree (Hons.) from NIT Jalandhar, India, in 2008, and the PhD degree from NIT Surat, India in 2013. He has been an Associate Professor at the Department of Electronics and Communication Engineering, Indian Institute of Information Technology, Design and Manufacturing, Jabalpur (IIITDM Jabalpur). At present, he is a Professor at Central University of Jammu (J&K). He had ten years of rich academic, industrial, and research experience in various institutes/universities, including NIT-Surat, Capgemini India Private Ltd., and SMVD University. He has published more than 101 journal articles out of which more than 61 SCI journal articles, including IEEE TRANSACTIONS, IEEE journal, Elsevier, Springer, Taylor & Francis, and Hindawi. He has published more than 25 interference including ITU-T, IEEE ANTS, INDICON, and APAN. He has filed eight patents out of which four are published. His research interests include wireless communication, power optimizations, wireless security issues, and optical fibre communication. He is a Senior Member of GISFI, SIAM, the International Association of Engineers (IAENG), the Advanced Computing and Communication Society (ACCS), and CSI. He has also served as an organizing member and a TPC member for several national and international conferences. He received the Young Scientist Author Award by ITU, in December 2010. He has received an APAN Fellowship, in 2011, Srilanka (2012), 2016, and China (2017), Singapore (2018), New Zealand (2018), South Korea (2019), and a Student Travel Grant from COMSNET 2012.

MANISH SABRAJ (Member, IEEE) received his Bachelor's degree in Electronics and Communication Engineering from Govt. College of Engg. & Technology Jammu affiliated with the University of Jammu in 2001. He received his M. Tech degree in Electronics and Communication Engineering from IIT Guwahati in 2003 and PhD in Electronics and Communication Engineering from Shri Mata Vaishno Devi University Katra (J&K) in 2013. He worked as a Lecturer from 2004 to 2008 and Asstt. Professor during 2008-2013. Presently, he is working as an Associate Professor at the School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University Katra,

 doi:10.20944/preprints202405.1066.v1

(J&K), India since 2013. His research interests include digital signal processing, digital communication, wireless communication and control systems.