UND School of Graduate Studies

GPS Anomaly Detection and Machine Learning Models for Precise Unmanned Aerial Systems Navigation

GPS ANOMALY DETECTION AND MACHINE LEARNING MODELS FOR PRECISE UNMANNED AERIAL SYSTEMS NAVIGATION

by

Jaya Preethi Mohan

Bachelor of Technology, Computer Science and Engineering,

Dr.M.G.R. Educational and Research Institute, 2019.

A Thesis

Submitted to the Graduate Faculty

of the

University of North Dakota

in partial fulfillment of the requirements

for the degree of

Master of Science

Grand Forks, North Dakota

December
2023

Name: Jaya Preethi Mohan

Degree: Master of Science

This document, submitted in partial fulfillment of the requirements for the degree from the University of North Dakota, has been read by the Faculty Advisory Committee under whom the work has been done and is hereby approved.

DocuSigned by:
Prakash Ranganathan
2E9D28B3432D4C6...
Prakash Ranganathan

DocuSigned by:
1EF0CCAE060C410...
Hassan Reza

DocuSigned by:
Wen-Chen Hu
EE71D88681C04D0...
Wen-Chen Hu

This document is being submitted by the appointed advisory committee as having met all the requirements of the School of Graduate Studies at the University of North Dakota and is hereby approved.

DocuSigned by:
Chris Nelson
2E0AF088C733403...
Chris Nelson
Dean of the School of Graduate Studies

12/7/2023
Date

PERMISSION

Title	GPS Anomaly Detection and Machine Learning Models for Precise Unmanned Aerial Systems Navigation
Department	School of Electrical Engineering and Computer Science
Degree	Master of Science

In presenting this thesis in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my thesis work or, in her absence, by the Chairperson of the department or the dean of the School of Graduate Studies. It is understood that any copying or publication or other use of this thesis or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of North Dakota for any scholarly use which may be made of any material in my thesis.

Jaya Preethi Mohan

20/11/2023

ACKNOWLEDGMENTS

I wish to express my sincere appreciation to the members of my advisory committee for their guidance and support during my time in the master's program at the University of North Dakota.

First and foremost, I am immensely grateful to my advisor, Dr. Prakash Ranganathan, for his invaluable guidance and expertise. His constructive criticism, valuable suggestions, and review of my work have significantly improved the quality of this thesis. His insightful feedback, patience, and dedication have shaped this thesis and helped me develop as a researcher. I am truly fortunate to have had his mentorship throughout my graduate journey.

I would like to express my gratitude to my thesis committee members: Dr. Hassan Reza, whose expertise in software engineering and software architecture has educated me in those domains, and Dr. Wen-Chen Hu, whose feedback and motivation have enhanced my programming skills from the beginning. I appreciate their time in evaluating my research.

My sincere thanks to the Federal Aviation Administration (FAA) for funding my research assistantship by supporting my research and student life. Thanks to my colleagues in the Center for Cyber Security Research (C2SR) team for their collaboration and support.

DEDICATION

To my mother in heaven, Jamuna Rani, thank you for your blessings throughout my life. I am forever thankful to my father Mohan Patchivannan and my brother, Harikesh Mohan, for being my support pillars. Thanks to Dr. Sumathy Eswaran (Former Dean of Dr. M.G.R. Educational and Research Institute) who encouraged me to pursue higher education.

List of Figures

List of Tables

Abbreviations

1. Global Positioning Systems (GPS)
2. Unmanned Aerial Systems (UAS)
3. False data injection (FDI)
4. False Data Injection Attack (FDIA)
5. Fifth-generation network (5G)
6. Federal Aviation Administration (FAA)
7. Airworthiness Directive (AD)
8. Internet of Things (IoT)
9. Vehicle to Vehicle (V2V)
10. Vehicle to Everything (V2X)
11. Vehicle or Building to Infrastructure (V2I/B2I)
12. Virtual Reality (AR/VR)
13. Confidentiality, Integrity, and Availability (CIA)
14. Radio frequency (RF)
15. Electromagnetic Compatibility (EMC)
16. Cyber-Physical System (CPS)
17. Inertial Measurement Unit (IMU)
18. Machine learning (ML)
19. Decision Tree (DT)
20. Hierarchical Clustering (HC)
21. Ordering Points to Identify Clustering Structure (OPTICS)
22. International Civil Aviation Organization (ICAO)
23. Enhanced Mobile Broadband (eMBB)
24. Massive Machine Type Communication (mMTC)
25. Ultra-Reliable Low Latency Communication (URLLC)
26. Silhouette Coefficient (SC)
27. David Bouldin's (DB)
28. Radio Access Network (RAN)
29. Device-to-device (D2D)
30. Multiple input multiple output (MIMO)
31. Quality of Services (QoS)

32. Network Functions (NFs)
33. Next-Generation Network (NGN)
34. Long-Term Evolution (LTE)
35. Augmented Reality (AR)
36. GPRS Tunneling Protocol (GTP)
37. Department of Defense (DoD)
38. Side-channel attacks (SCA)
39. User Equipment (UE)
40. Kilowatt (kW)
41. Cybersecurity and Infrastructure Security Agency (CISA)
42. National Cybersecurity Centre (NCSC)
43. National Institute of Standards and Technology (NIST)
44. Distributed Denial of Service (DDoS)
45. International Mobile Subscriber Identity (IMSI)
46. Radio Access Networks (RAN)
47. GPRS Tunnelling Protocol (GTP)
48. Standalone (SA)
49. Multi-access Edge Computing (MEC)
50. Public Key Infrastructure (PKI)
51. Density Based Spatial Clustering (DBSCAN)
52. Ordering Points To Identify the Clustering Structure (OPTICS)
53. Gaussian Mixture Models (GMM)
54. Hierarchical Clustering (HC)
55. Silhouette Coefficient (SC)
56. Dallas Fort Worth (DFW)

Table of Contents

ABSTRACT

The rapid development and deployment of 5G/6G networks have brought numerous benefits such as faster speeds, enhanced capacity, improved reliability, lower latency, greater network efficiency, and enablement of new applications. Emerging applications of 5G impacting billions of devices and embedded electronics also pose cyber security vulnerabilities. This thesis focuses on the development of Global Positioning Systems (GPS) Based Anomaly Detection and corresponding algorithms for Unmanned Aerial Systems (UAS). Chapter 1 provides an overview of the thesis background and its objectives. Chapter 2 presents an overview of the 5G architectures, their advantages, and potential cyber threat types. Chapter 3 addresses the issue of GPS dropouts by taking the use case of the Dallas-Fort Worth (DFW) airport. By analyzing data from surveillance drones in the (DFW) area, its message frequency, and statistics on time differences between GPS messages were examined. Chapter 4 focuses on modeling and detecting false data injection (FDI) on GPS. Specifically, three scenarios, including Gaussian noise injection, data duplication, data manipulation are modeled. Further, multiple detection schemes that are Clustering-based and reinforcement learning techniques are deployed and detection accuracy were investigated. Chapter 5 shows the results of Chapters 3 and 4. Overall, this research provides a categorization and possible outlier detection to minimize the GPS interference for UAS enhancing the security and reliability of UAS operations.

CHAPTER 1
INTRODUCTION

1.1 Motivation

Global Positioning Systems (GPS) produce messages with several features: time, positional information containing latitude, longitude, speed, and number of satellites used[1]. A rising number of hazards, such as solar activity, man-made interference, malicious spoofing or jamming, and manipulation of timestamps can affect the integrity of GPS and its reliant systems. GPS systems on vehicles are vulnerable to spoofing through false data injection attacks (FDI) that impact vehicular localization and navigation [2]. The cyber security attacks targeting the time field records may take many forms: replay attacks, duplication, intentional delay insertion, etc. in any GPS relying on Cyber-Physical Systems [3]. On the other side, the fifth-generation network (5G) is an emerging technology for dynamic applications, but it is still exposed to vulnerabilities and incompatibilities with major operations like aviation. The Federal Aviation Administration (FAA) revised the landing specifications for specific Boeing 737 series aircraft at airports where 5G interference may occur in an Airworthiness Directive (AD). Landings at airports where the FAA concluded that the aircraft radio altimeters are safe and reliable in the 5G C-band environment are not subject to the AD. Additionally, it does not apply in airports without 5G deployment. The FAA issued the AD because several Boeing 737 systems rely on the radio altimeter, including auto throttle, ground proximity warning, thrust reversers, and Traffic Collision Avoidance System. The AD takes effect immediately after it is published in the Federal Register and affects about 2442 aircraft and in the United States and 8,342 in other countries[4]. The fifth-generation mobile network (5G) services have the potential to provide high-speed connectivity to a large user base with excellent benchmarks on low latencies, large capacity, and faster upload/download data rates. The potential for millimeter-wave technologies

to sustain enough power for mobile/Wi-Fi connectivity for indoor/outdoor applications provides an additional layer of expansion of 5G services to enhance good user experiences. The probability of a threat landscape increases with a significant increase in network connectivity, users, non-existent or non-compliant Internet of Things (IoT) standards, and service types. Network mobility and applications that are planning on deploying 5G services such as Vehicle to Vehicle (V2V), Vehicle to Everything (V2X), Vehicle or Building to Infrastructure (V2I/B2I) Augmented and Virtual Reality (AR/VR), digital twins-based and streaming video services increase vulnerabilities and risk landscape compromising Confidentiality, Integrity, and Availability (CIA) properties.

When an electronic device is near an electromagnetic field in the radio frequency (RF) range, it can experience electromagnetic interference, which causes it to malfunction. Strong RF fields cause a lot of electronic gadgets to malfunction. The disruption may delay, or otherwise reduce or limit the circuit's performance to function effectively. Any object manufactured or natural, that carries electrical currents that change quickly can serve as the source. The ability of systems, equipment, and devices that make use of the electromagnetic spectrum to operate in their intended operational environments without experiencing unacceptable degradation or inflicting unintentional degradation due to electromagnetic radiation or response is known as electromagnetic compatibility (EMC). It uses electromagnetic spectrum management, the setup of systems, equipment, and devices to assure interference-free operation, and understandable concepts that enhance operational efficiency. According to National Security Telecommunications and Information System Security (NSTISS) 1993, Electronic and electromechanical information-processing equipment can produce unintentional intelligence-bearing emanations, commonly known as TEMPEST. If intercepted and analyzed, these emanations may disclose information transmitted, received, handled, or otherwise processed by

the equipment. in other countries[5]. The disruption may delay, or otherwise reduce or limit the circuit's performance to function effectively.

Any object manufactured or natural, that carries electrical currents that change quickly can serve as the source. The ability of systems, equipment, and devices that make use of the electromagnetic spectrum to operate in their intended operational environments without experiencing unacceptable degradation or inflicting unintentional degradation due to electromagnetic radiation or response is known as electromagnetic compatibility (EMC).

It uses electromagnetic spectrum management, the setup of systems, equipment, and devices to assure interference-free operation and understandable concepts that enhance operational efficiency. Fig 1 represents the potential for 5G signal interference and cyber security attack

Fig. 1. 5G signal interference and cyber-attack with UAS types

1.2 Related works

In the UAS environment, GPS is highly exposed and that leads to several consequences. (A. Afaq.,) proposed an architecture to detect jamming attack in 5G networks using machine learning algorithms.

5G security-based research[6] is potential for cyber security attack detection. used the multiple clustering models to detect anomalies from jamming attacks, and cyber-physical attacks through Reinforcement Learning, classification, and regression algorithms in their proposed architecture. GPS data is used for detecting anomalies from cyber security attacks such as spoofing attack, GPS jamming and intrusion detection in the UAS flights through machine learning algorithms[7][8] which influences the applications of unsupervised and supervised machine learning methods on GPS data to separate the anomalies and predict the risk level of GPS dropout. The existing research on real-time machine learning models has discussed the uses of mathematical models, artificial intelligence, data modeling fuzzy logic and image analysis for anomaly detection.

Unmanned Aerial Systems have been construed as a Cyber-Physical System (CPS) [9] UAS contain sensors, communication, and computational elements such as microcontrollers. UAS uses data extracted from sensors (e.g., IMUs, gyroscopes, accelerometers, battery, GPS, antennas or other payloads) for navigation, communication, and flight control. Anomalies in the data extracted can impact UAS performance leads to flight instability, causing the vehicle to crash, and destroy its mission[9].The authors in [10] discuss how DJI Matrix 100 UAS can be attacked using a simple software defined radio (SDR) setup using HACKRF. They modeled a GPS spoofing attack to mimic the GPS coordinates of a geo-location. The Kalman filtering method were used to detect anomalies in the spoofed GPS dataset. False Data Injection Attack (FDIA) compromises the integrity of the system with inaccurate information.

In [11], the authors modeled a false data injection attack with fuzzy logic in trapezoid and sigmoid shape scenarios to falsify the home area network sensor data. The detection phase used multiple machine learning (ML) models and artificial neural networks (ANN) were seen as the best model to detect false data injection attacks in power systems. Dynamic Data Aware Firefly-based clustering was used to detect the FDI on the Internet of Things (IoT) sensor data [12]. Deep learning methods improvement for the FDI detection rate problem in transportation systems over Logistic Regression, Support Vector Machine, and Conventional Neural Network[13]. According to (V. Zeufack), unsupervised machine learning and supervised machine learning models are emerging as promising algorithms to detect cyber-attacks in the Power grid [14]. Hierarchical clustering and Decision Tree (DT) based regressor methods also has a good probability of detection rates with respect to denial-of-service attacks (DoS) and FDI attacks. Hierarchical Clustering (HC) algorithms performs better over Kalman Filtering technique. The Ordering Points to Identify Clustering Structure (OPTICS) algorithm was used to identify the anomalies in the *log files* for a system [15]. This method is applied to the streaming data and evaluated with metrics such as F-1 score, precision, and recall. The centroid of the OPTICS cluster shows anomalies clearly over normal data.

UAS are utilized in various applications after the declaration of Part 107 rules. The promulgation of this rule improved the UAS utilization, widened the UAS administration and licensure. In the airport regions, the UAS have been used for various applications such as obstruction analysis, airfield light inspections, security emergency response, pavement condition assessment and airport inspections [16] [17]. DJI aeroscope is a device that detects a drone with radio frequency (RF) detection method, direction finder (DF) configurated antennas 4, 8, or 16 antenna array placements and the Internet connected receivers[18]. The authors in [19], uses DJI aeroscope data on UAS position logging equipment analysis and stated that packet sniffing technology

captures the dataflow through network. DJI aeroscope were deployed and collected data for 30 days of period at Daytona Beach International Airport [20]. An intrusion detection framework was developed for invasive FPV drones using video streaming characteristics as another approach for drone detection and authentication purposes [21]. An Automatic Dependent Surveillance-Broadcast (ADS-B) device broadcasts flight state information such as position, velocity, and identification number, which carries more information through broadcast datalink depending on air traffic [22].

The authors analyzed the conflicts between an equipped aircraft and UAS in the Orlando Melbourne International Airport. Unauthorized drone activities have disrupted the airport operations and lead to the loss of 5 and 60 € million per incident. ADS-B data evaluation is a surveillance method for air traffic management (ATM) recommended by the International Civil Aviation Organization (ICAO).

The global navigation satellite systems obtain the position information of the ADS-B report[23]. The research findings influence the data analysis of flight logs from DJI aeroscope, ADS-B receiver and GPS sensors data receivers. Multiple supervised machine learning models were used in the research [24] to classify and detect the GPS signals affected by spoofing attack. From the observation of various research findings, there is a research gap in identifying the risk level of UAS time difference. It is essential to measure the time difference of various drone types to understand the GPS reliability through UAS data receivers. In this thesis, we have analyzed the DJI aeroscope data captured for surveillance that detected multiple drones and their drone types used for surveillance purpose. Each drone has its own time difference value between each message recorded and in different time windows. We categorized the analysis methodologies into three different methods such as statistical analysis, and risk classification through machine learning models.

1.3 Research Objectives

In this work, we identify GPS dropouts, model false data injection and classify the risk level of GPS dropouts.

1. Categorize the cyber and non-cyber-attacks that occur on the major 5G network services and identify the attack consequences and likelihood with mitigation strategies.

2. Model a false data injection attack for multiple scenarios such as data duplication and data manipulation. The use of unsupervised machine learning algorithms to analyze and detect the false data injection attack.

3. Classify the risk level of GPS message dropout on the DJI aeroscope sensor dataset.

1.4 Thesis Organization

Chapter 1 discussed the problem statement and research objectives. It also introduces the importance of GPS anomaly detection for Unmanned Aerial Systems due to the vulnerabilities from the cyber and non-cyber perspective.

Chapter 2 provides a high-level categorization of cyber-attacks related to 5G environment into Physical, Remote, and Local. The various benchmarks (latency, bandwidth) for 5G network evaluation across multiple 5G related technologies such as Enhanced Mobile Broadband (eMBB), Massive Machine Type Communication (mMTC), Ultra-Reliable Low Latency Communication (URLLC) Rapid demand for bandwidth and high mobile traffic burdening existing 3G/4G network performance to be slower and unreliable to many new emerging services.

Chapter 3 models one such dropout scenario by injecting false data into original GPS timestamps representing interference. We inject ‘dropouts’ via insertion of false data, and duplicating time stamps. The end goal is to investigate the performance of FDI detection using several clustering algorithms: 1) Density-Based Spatial Clustering, 2) Ordering Points to Identify the Clustering

Structure, 3) Gaussian mixture models, and 4) Hierarchical Clustering. Multiple grouping indices such as Silhouette Coefficient (SC) and David Bouldin's (DB) Index were used to evaluate normal vs. abnormal points grouping. The chapter also investigated non-clustering approach such as Isolation Forest, which seems to be a better candidate for such FDI detection.

Chapter 4 discusses the time difference analysis of DJI aeroscope surveillance data with statistics, risk labeling, and classification of risks with machine learning models and its evaluation metrics.

Chapter 5 shows the results obtained from Chapters 4 and 5 for GPS anomaly detection and risk classification. All the codebase for the research can be found on the link.

CHAPTER 2
CYBER SECURITY THREATS FOR 5G NETWORKS

In 5G networks, devices such as smartphones are connected through an important part of a cellular network infrastructure called Radio Access Network (RAN), which allows integrating and improving the network utilization of mobile devices [25]. Device-to-device (D2D) communication is a "network of networks" in which multiple networks are integrated for data services and network communication over radio access technologies [26]. The network architecture comprises three different layers: *infrastructure, control, and application* layers. Each layer differs by the type of component placements and varying degrees of functionalities. All the connection types in the 5G network are linked to multiple input multiple output (MIMO), which is a technology to multiplies the capacity of a radio link by relying on arrays of transmission and receiving antennas to exploit multi-path propagation [27]. 5G was introduced by the 3rd Generation Partnership Project (3GPP) to expand the quality of services (QoS) and enhance user experiences. It is designed to support a larger number of networks connected devices with high data volume, and low latencies than 4G networks [28]. Fig. 1 represents the different download speeds of the recent 3 cellular network generations [29].

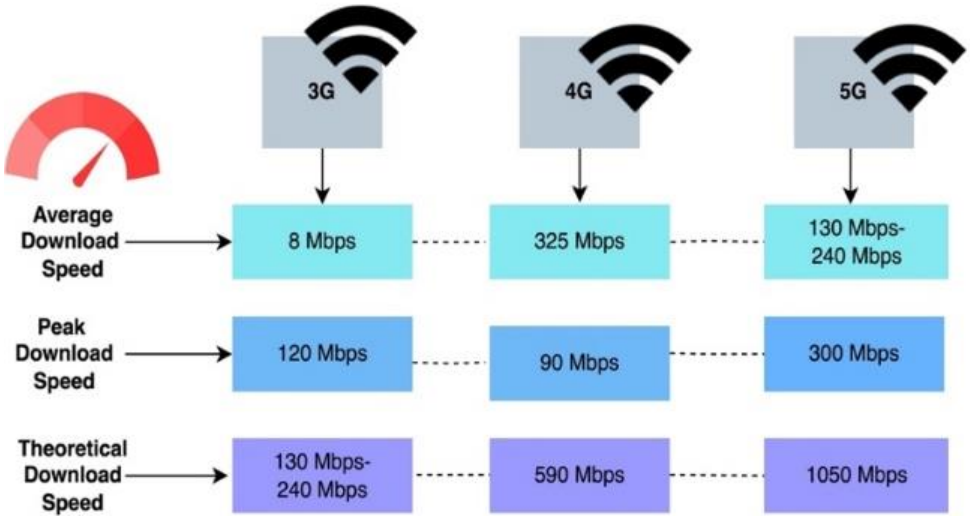


Fig. 2.Download speeds for 3G, 4G, and 5G.

The connectivity components like routers, switches, and base stations are placed in the *infrastructure* layer. The control layer implements the decision-making entities and network control function that is integrated into the application layer. Network services are utilized, and business applications are executed in the application layer [30].

Massive machine-type communication (mMTC) is communication carried by machine or software platforms for coordinating, sensing, and actuation that is not operated by humans [31]. 5G can reduce the MTC latencies to 1 millisecond (ms) between wireless devices. This is a significant improvement from the latencies of 50 ms and 60 ms for 3G and 4G technologies respectively [32].

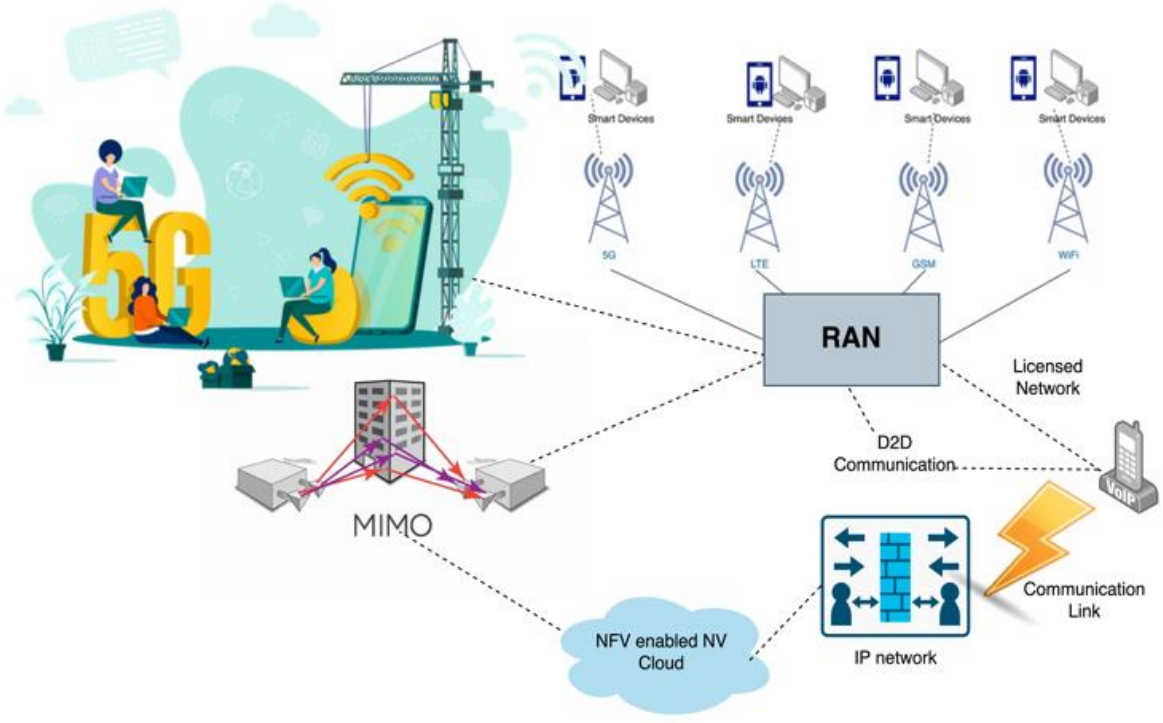


Fig. 3 5G Network Architecture

Machine-type communication enables 5G services to operate securely, reliably and autonomously [33]. AT&T and FirstNet network organizations collaborated to provide public safety or emergency responder-based services using 5G networks [7]. AT&T also experimented several trials using milli-meter-wave (mmWave) technology in Austin, Texas to evaluate

network capacity, speed, and latency [34]. Table 1 highlights the global trends or incidents in the 5G space, observed or predicted consequences, and quantitative findings/projections for the respective trend. The major security issues currently being faced by 5G network operators are supply chain weaknesses, espionage of 5G technology's corporate secrets, high-scale deployment of edge devices, and vulnerabilities in network functions (NFs) such as network slicing.

Table 1 Notable 5G security trends

Threats/Trend	Consequence(s)	Significance	Reference
4G and 5G Vodafone Networks Exploited by Hackers	**Disruption and Shut Down** of Networks and Network Resources.	4,000,000 Affected for 24+ Hours.	[35], [36]
Cyber Espionage by State Sponsored Cyber Groups Targeted at Telecom Providers	**Data Espionage** of Sensitive or Classified Information	23 Telecom Providers Compromised Across 3 Continents	[37]
High Volume Deployment of Internet of Things (IoT) Devices	Compromised Devices Susceptible to **DDoS and SCA Attacks**	1 million Devices Projected per Unit Area	[38][39]
Improper Separation of Network Slices using Cloud Technology	**Cloud-based** Vulnerabilities are Transferred to Network Slices	-	[40]
Major Suppliers of Telecom Equipment are Based in China	**Vulnerabilities and Backdoors** for Remote Monitoring	70% of the Chinese Telecom Market is State-owned	[41]

2.1 5G Network Requirements and Services

According to ITU-R, 5G comprises of three major services: Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC), and Ultra-Reliable and Low Latency Communications (URLLC). Each service supports 5G in various prospective for efficient usage of network resources [12].

- **Enhanced Mobile Broadband (eMBB)**

Next-Generation Network (NGN) aims to build a network combining different wireless networks in a complex structure for wide broadband usage. The Long-Term Evolution (LTE) network is the current technology for mobile data communication. LTE is a standardized network that supports 5G services with low latency and high broadband capacity. The enhancement of mobile broadband service (eMBB) aids in faster data rates (20 Gbps), low latency (in the order of 7 ms), and enhanced user experiences [42][43]. It offers support to various multimedia streaming environments such as augmented reality (AR), virtual reality technologies, and high-definition video streaming.

- **Massive Machine Type Communication (mMTC)**

mMTC aids in the advancement of IoT technology and enables the realization of smart cities, smart grids, autonomous vehicles, smart buildings/ transportation, and precision agriculture environments. It also provides low power consumption and high reliability. mMTC can support ten 10 years of battery life with a single charge and a coverage density of a million devices in a single sq. kilometer [44]. mMTC is applicable in IoT for sensors, transport systems, smart city, manufacturing, and staff control areas.

- **Ultra Reliable Low Latency Communication (URLLC)**

URLLC is one of the major services of communication for packet delivery and data transmission. There are strong network requirements for this communication service under factors such as availability, reliability, and latency. It fits into the development of evolving applications and services. The major applications are industrial automation, vehicular communication, and manufacturing sectors. It plays a vital role in the telecommunication sector for user experience and business development. The working group of 3GPP RAN focuses on a communication

service of the design Rel-15 that provides low-level payloads i.e., 32 bytes and 1ms radio latency. URLCC is fast and transmits data consistently which is preferable for transport, manufacturing, and healthcare. The service prioritizes low latency, high reliability, and low probability of error. For applications like automated vehicles, remote control industries, diagnostics, robotic surgery, and telemedicine. The probability of error should be between 10^{-5} and 10^{-8} and latency less than 3ms [45][46].

2.2 5G Spectral Band Specifications

The spectral bands can be grouped into licensed and unlicensed bands. The radio spectrum band is an important allocation that separates critical (military) and non-critical (civilian) applications for growing wireless communication needs. Telecommunication operators provide high band to a service with broad coverage, selecting appropriate channel coding and high-speed networks for many users [47]. 5G produces its agility and a new range of flexibility to satisfy user needs on connectivity and service capability.

- **eMBB Radio Band**

Band level: Low-band

The frequency range coverage is extensive in the low-band spectrum of a 5G network. This radio band of eMBB is suitable for regions that are densely populated or urban environments. The download speed of a low-level radio band is 20 Gbps and 20 times the latency network. eMBB is preferred in streaming applications that demand high data rates Examples of applications include AR/VR, private broadband services, and high-definition video streaming.

- **URLLC Radio Band**

Band level: Mid-band

URLLC services use mid-band spectrum which can support mission-critical systems, services or applications. The end-to-end latency for this band is less than 5ms and it has a 99.9%

uptime. Applications for this band include Vehicle-to-everything (V2X), automated vehicles, smart grid, unmanned aviation, remote medical procedures, and industry automation.

- **mMTC Radio Band**

Band level: High-band

mMTC Radio band is suitable for IoT based applications or devices. This band is suitable to realize applications such as smart cities, smart grids, smart homes, etc., where there is a need for large collection of low-powered embedded sensors or devices that need to be connected and supported for network communication.

2.3. Potential Cyber Attacks

Cyber threats to 5G infrastructure can broadly be classified into two attack types: passive and active. Passive attacks such as eavesdropping and traffic analyses [48] do not intervene in a network's traffic to modify, insert, or delete data but passively monitor the data being transferred; they do not alter the system states or data [49]. Cyber security properties such as confidentiality, integrity, and availability (CIA) of 5G networks require multi-layered authentication to thwart threats. Active attacks like jamming, sybil, spoofing, impersonation, man-in-the-middle, and denial of service are carried out to alter systems and their data by compromising the integrity, confidentiality, and availability to cripple operational systems, and to steal or manipulate valuable data.

The authors have grouped the potential cyber-attacks into possible likelihood of occurrence and its impact on 5G services. This paper categorizes attacks as follows (please see Fig. 3):

A. Remote Attacks

B. Local Attacks.

C. Physical Attacks.

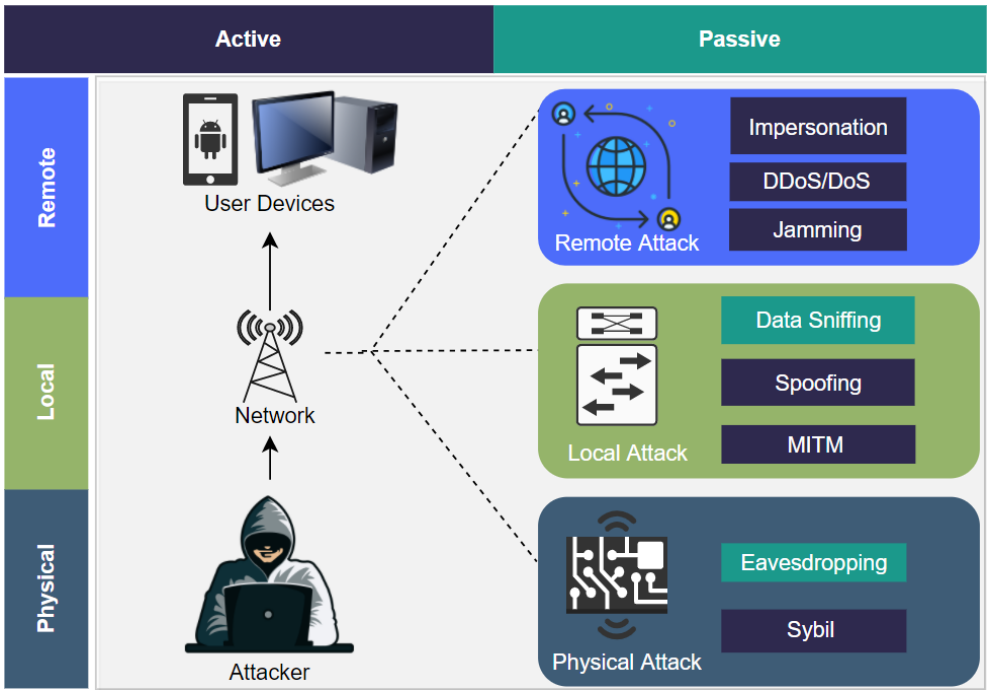


Fig. 4. Cyber threat categories: physical, local, and remote.

Remote Attacks

- Vulnerabilities in the GPRS Tunneling Protocol (GTP), can be exploited by remote threat actors to impersonate users using details such as authentication status, location, and subscriber settings [50].
- DDoS and DoS attacks can be launched by a malicious NF against a legitimate NF as there is no authentication mechanism to verify the identity of a NF [51].
- Jamming is an attack that disrupts the signal of the physical devices from input and output transmission. mMTC Scenario: Data transmission in IoT terminals [52].
- Jammers use wireless and cellular 5G networks to attack critical infrastructures and public safety services. Several types of jammers [53] and jamming techniques [54] can be used to attack 5G networks.

Local Attacks

- Local area network (LAN) and wireless local area network (WLAN) can be accessed with an open base station through unauthorized users on the network [55].
- Smart grid applications and network slicing [56] are scenarios that can be exploited.
- A man-in-the-middle attacker can create a fake 5G base station to act as a relay between the user and the 5G core network to intercept sensitive information [57][58].
- Local area network (LAN) and wireless local area network (WLAN) can be accessed with an open base station through unauthorized users on the network [55].

Physical Attacks

- Resilient physical-layer defenses to eavesdropping attacks remain an open issue that warrant further research [59].`
- Attacker's intercept and analyze traffic on the device communication link that transmits critical communication signals, ligament information includes device and the risk and network configuration details will lack privacy protection.
- Scenarios: eMBB software defined network (SDN) and IoT device.
- According to Rahimi and colleagues [60], sybil attacks can be carried out at the connectivity layer which handles the device-network communication.

Based on the extensive literature review, the authors subjectively assess the impacted services and corresponding risks levels as outlined in Table 2.

Table 2 Potential cyber threat vectors for 5G networks.

Attack Type and Description	**Attack / Loss of CIA Property**	**Remark(s)**	**Impacted Service(s)**	**Risk Level/ Impacts**	**References**
Remote Attack: Attacks initiated wirelessly or through the Internet	Impersonation (Confidentiality & Integrity)	a) Openness of a wireless channel allows the attacker to perform remote attacks by tracking and controlling the communication channel.	eMBB Scenario: Falsification in network slicing	↔ (Medium)	[25][40] [41], [42][43] –[45]
		b) Impersonation attacks can be carried out even without prior knowledge of a user's credentials or if an adequate authentication mechanism is not implemented	mMTC Scenario: Access denial of legitimate user(s)		
	DDoS/DoS (Availability)	a) High bandwidth and low latency of 5G increase the likelihood of DDoS attacks [46].	eMBB Scenario: Access denial in network slicing.	↑ (High)	[33] [31][25] [34] [47], [48] [49], [50]
		b) DDoS attackers target central control units to scale the attack to large servers or networks. This is carried out on the network layer to stop the user services.			
		c) Combination of DDoS and DoS can attack virtual NFs to disrupt host services network.			
	Jamming (Availability)	Jammers use wireless and cellular 5G networks that are majorly implemented in public safety services. Several types of jammers exist for attacking 5G networks.	Scenario: Jamming on IoT devices.	↓ (Low)	

Local Attack: Attacks within local area networks (LANs)	Data Sniffing (Confidentiality & Integrity)	a) Data sniffing takes place in the virtual local area network (VLAN) of link-layer within LANs	URLLC Scenario: Smart grid applications and network slicing.	↔ (Medium)	[23][34] [35][36] [51] [30] [52]–[54][48], [55], [56]
	Spoofing (Confidentiality & Integrity)	b) LAN and WLAN can be accessed with an open base station through unauthorized users on the network		↑ (High)	
	Man-in-the-Middle (MITM) (Confidentiality & Integrity)	c) User messages are tracked by monitoring communication channels.	URLLC Scenario: IP spoofing.	↔ (Medium)	
		d) The communication data between two legitimate parties are replaced or modified by attackers to obtain confidential data.			
Physical Attack: Attacks requiring physical hardware access	Eavesdropping (Confidentiality & Integrity)	Eavesdropping attacks may happen on the physical layer of the 5G network by intercepting and analyzing traffic to access confidential data (i.e., identity, authentication credentials, location).	eMBB Scenario: SDN and IoT device.	↑ (High)	[57] [31][36] [47][58] [59] [60] [61][62] [63]
	Sybil (Integrity)	Sybil attacks create fake identities and inject false information to get and maintain access to a physical device.	mMTC Scenario: Data transmission in IoT terminals and Vehicular control.	↓ (Low)	

2.4 Cyber and Non-Cyber Risks in 5G Networks

5G poses serious cyber risks (if not addressed) regardless of the spectrum band usage in any network type. A recent US Department of Defense (DoD) report shows that the code used for the base station is secure and permitted for telecommunication vendors to access, but the network infrastructure or security equipment (firewalls or routers) is vulnerable to anonymous activity as they come from third-party vendors. Lack of regular maintenance or software updates or patches could expose new vulnerabilities within the infrastructure [36][28]. 5G networks are not only vulnerable to risks that compromise the CIA properties of the infrastructure and communicating parties, but also bring concerns related to power consumption, and supply chain vulnerabilities.

5G network capability plan to support tens of billions of IoT devices worldwide and 7.6 billion smartphone users in the next decade. 5G's network power consumption will exceed exponentially although bits per kilowatt (kW) remains lesser. With the penetration of several small cell technologies, the user capacity demand is to go to surge to accommodate large users and energy or vehicular/building infrastructure networks (V2X, V2I). As portable small cell networks may rely on chargeable lithium-ion batteries, relying on conventional fossil fuel-based electricity is not sufficient. Thus, portable and scalable renewable energy resources are required to address power generation and resource efficiency [86].Power consumption rate has gradually increased from 3G, 4G, and 5G: there was a 43% increase of power consumption from 3G (4808 W) to 4G (6877 W) and a 68% increase from 4G to 5G (11,577 W) [87]. A significant part of 5G's user equipment (UE) will consist of IoT devices and side-channel attacks (SCA) based on power characteristics pose a threat to user privacy.

Timing-based side channel attacks [88] analyze the interference produced during regular device traffic to identify patterns in device behavior. Such attacks can probe deeper to gather data such as device type, device-user interactions, and the no. of people using the device(s). Another type

of SCA called profiled SCA is regarded as the most dangerous type of SCA as it assumes that a threat actor has access to a cloned IoT device [89].Supply-chain components used in the development of 5G infrastructure and the policies/standards that are meant to ensure minimum performance and reliability requirements can indirectly or directly contribute to the exploitation of 5G networks.

According to CISA's 5G Strategy [90] for the United States, there is a strategic initiative to ensure that "state-influenced" entities do not dominate the 5G market partially because the low upfront costs associated with the procurement and deployment of 5G components will snowball into long-term expenses that will inevitably have to address security flaws in 5G's hardware and software architecture. A report from ETH Zurich [91] highlights the importance of a comprehensive analysis of 5G equipment before deployment. This is due to the economic power shift in the manufacturing of 5G equipment from the US to other countries like China. The UK National Cybersecurity Centre (NCSC) reports that Huawei performs poorly due to sub-par software source codes that are rife with software bugs. Further investigation points out that this observation is not specific to Huawei; European manufacturers like Ericsson and Nokia are also noted for having software vulnerabilities in 5G equipment that can be exploited by malicious actors.

2.5 5G Threat Surfaces

5G, at its inception, was expected to build upon existing 3G and 4G/4G (LTE) infrastructure to provide low latency and high-speed services to applications in transportation, aviation, automotive, and energy domains. However, 5G is not without its weaknesses and can be exploited by its threat surfaces. A threat surface, as defined by the National Institute of Standards and Technology (NIST) [92], consists of "the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data

from, that system, system element, or environment." For example, disruption to aviation services due to 5G services are emerging and causing mass schedule changes and cancellations. According to FAA [93], as 5G infrastructure uses new frequencies, increased power levels, and warrants closer proximity of flight operations, existing aviation equipment's (e.g., radio altimeter equipment closer to antennas) are noticing disruptions to airport operations, and thus warrants restrictions. Such equipment's could also be attacked by a hacker through side-channel attacks by emulating "potential cyber-attacks" as disruptions through any of the attack type (Physical, Local, or Remote) categories. Similar threats exist to other critical infrastructures such as U.S. Power Grid assets (i.e., transmission/distribution lines, substations, circuit breakers, relays, phasor measurement units, Distributed Energy Resource (DER's) controllers), Gas Pipeline Networks (e.g., pumping stations/junctions, switches), and Water/Sewage or Storm Treatment Systems (e.g., key interconnect units or switches). Several IoT devices are being manufactured with no cybersecurity measures and provide several backdoors for vulnerabilities (e.g., man-in-the-middle attack) to exist.

- **Hardware**

The hardware threats can be characterized by endpoint devices such as remote terminal units (RTUs), firewalls, sensors, and power infrastructure. These devices can be considered part of 5G's hardware ecosystem and rely on 5G services to provide improved and more reliable performance. Additionally, 5G moves its core functions like data storage to edge devices and sub-systems like those within autonomous vehicles in the V2X paradigm to introduce additional attack surfaces [94].

5G infrastructure is being integrated with current 4G LTE networks [95] and is susceptible to attack vectors such as distributed denial of service (DDoS). Soldani [96] lists assets (anything that is of value to an organization or an individual) in the 5G system, such as firewalls, radio

access networks (RAN), and UE to be vulnerable to cloning, hijacking internet of things (IoT) devices to create botnets, and international mobile subscriber identity (IMSI) catching.

- **Operations**

Operations-side processes include supply chain components used in the design of 5G infrastructure and its policies or standards that are meant to ensure minimum performance and reliability requirements. The Cybersecurity Infrastructure and Security Agency (CISA) [97] highlights the risk of purchasing and deploying components produced by international suppliers: risks such as the insertion of malware and backdoors, and manipulation of sensitive components can expose a nation's broader 5G network to attack vectors. While manufacturers such as Intel, MediaTek, Huawei, and Qualcomm have most of the market share when it comes to proprietary 5G-compatible hardware, it compels customers and vendors to implement features within these technologies that are not standardized by policies and are thus optional. This could introduce new vulnerabilities or attack vectors in the client networks that may be specific to manufacturers.

- **Network**

According to Positive Technologies [98], most 5G deployments in 2020 were non-standalone (NSA) and used the Diameter protocol (also called Diameter Signaling protocol) and GTP). Diameter is used to exchange subscriber profile information such as location updates, subscriber data, voice, or video sessions, user authentication, quality of service, and mobility requirements. This section classified three threat surfaces to 5G infrastructure: hardware, operations, and network as shown in Fig. 4. Diameter is an industry-standard protocol used in 4G LTE networks for authentication, authorization, and accounting (AAA) purposes while GTP is used primarily to "tunnel" or route internet protocol (IP) packets initiated from a source IP address (mobile device) to a destination IP address (target webserver) through the cellular network's core

segment. Both these protocols have open vulnerabilities that can be exploited. The 5G standalone (SA) architecture accommodates multiple features such as a distributed cloud-based core network, SDN and network function virtualization, and multi-access edge computing (MEC) [38]. While these features offer multiple benefits, security issues can lead to unauthorized access, configuration errors, and exposure to third-party vulnerabilities.

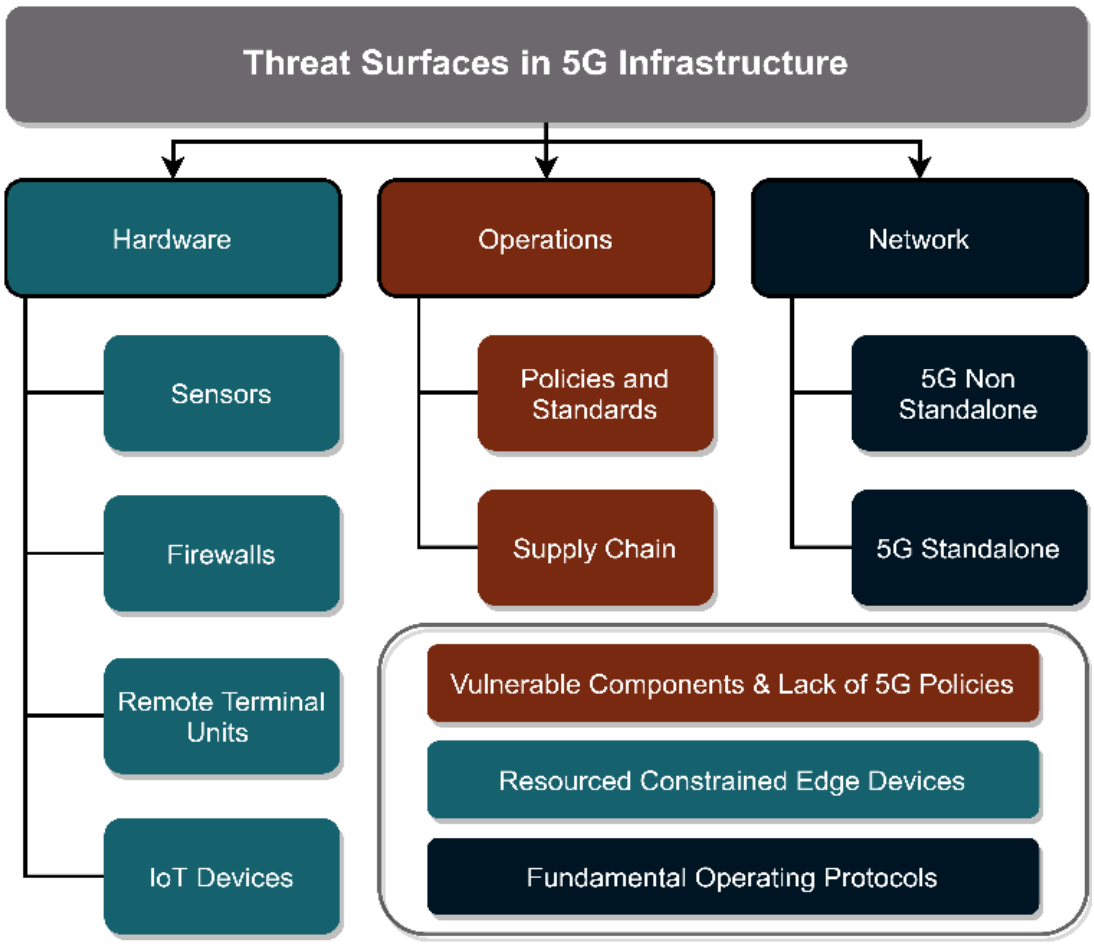


Fig5.5G infrastructure vulnerable components.

2.6 Countermeasures

Based on findings in Section IV, the following cyber-attacks pose as threats to 5G deployments, namely: impersonation, DoS/DDoS, sybil, eavesdropping, data sniffing, man-in-the-middle,

spoofing, and jamming. Table 3 summarizes the countermeasures and subclassifies them as either prevention or mitigation tactics.

Table 3 Countermeasures for cyber-attacks on 5G networks

Attack	Countermeasures	Prevention (P)/ Mitigation (M)	Reference
DoS/DDoS	Setting thresholds for transmitted traffic, stress tests, and adequate capabilities to handle peak network requests	P/M	[78][77]
Spoofing	Timing blacklists, authentication mechanisms	P/M	[79]
Man-in-the-middle	Access control policies, symmetric/asymmetric encryption	P	[80]
Jamming	Channel monitoring, jammer timing patterns, relay schemes	P/M	[31]
Eavesdropping and Data Sniffing	Hardware modules (eSIM), symmetric/asymmetric encryption	P	[78][81] [82]
Sybil	Blockchain networks prevent the creation of multiple fake identities, certifying authority to verify identities	P	[83][84]

Prevention tactics are implemented before the network has been subject to a cyber-attack whereas mitigation measures lessen the implications of a cyber-attack. Rosenblatt [100] from the Yale Cyber Leadership Forum advises the regular application of “stress-tests”: tests that simulate attacks such as DoS/DDoS at various threat surfaces of a 5G network to assess the magnitude of these attacks and implement adequate backup measures. Spoofing attacks can be mitigated by setting a countermeasure that prevents any suspicious agent from accessing 5G functions. timers can be used to blacklist certain agents from accessing the network if there is no response after predefined periods [101]. Additionally, there should be tactics in place that ensure that the

participating parties (base stations and end devices) are legitimate prior to initiating cellular connections and executing certain procedures.

Man-in-the-middle attacks can be countered by enforcing adequate access control measures to prevent unauthorized modification [102]. Ensuring that data are encrypted by a strong public key infrastructure (PKI) mechanism will protect relayed data from being decrypted by a man-in-the-middle attacker. Jamming attacks can be detected by monitoring the network for any excess or sudden change in a specific 5G channel by metrics such as bit error rate and setting thresholds to distinguish normal and anomalous channel behaviors. Eavesdropping and data sniffing attacks can be mitigated by using encrypted network data [99]. To complement this measure, it is advised to assign encrypted temporary identities to connecting devices and regularly update this information to prevent user tracking. Preventing sybil attacks primarily involve methods to ensure the legitimacy of the participants in the network. According to Coin Central [105], using a blockchain to increase the cost associated with creating identities in a 5G network will limit the number of fake or malicious users executing a sybil attack.

2.7 Conclusion

This chapter provides a review of potential cyber-threat vectors into three categories: Physical, Remote, and Local. Further, several threat vectors can also be classified into Hardware, Operations, and Network types. As demand for more spectrum will surge, it is natural for the cyber threat landscape to grow. As telecommunication companies or network providers have begun to deploy 5G services, it is important to assess the security exploitations early on across the three categories to avoid expensive re-design/re-installations of 5G infrastructure that may hinder both critical (i.e., energy, aviation, water/sanitary systems, and transportation networks), and non-critical (user authentication and privacy challenges) infrastructures. Futuristic mitigation solutions (e.g., blockchain, encryption mechanisms, multi-layered credential or policy

authentication, access privileges to key resources) should be carefully designed and must be robust to track and deter threats as this technology is new and evolving. The following chapter will model the GPS timestamps and deploy multiple clustering methods as the mitigating approaches. This is the use case of a cyber security attack on 5G networks.

This chapter was published as a research manuscript in IEEE digital explorer.

J. P. Mohan, N. Sugunaraj and P. Ranganathan, "Cyber Security Threats for 5G Networks," 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 446-454, doi: 10.1109/eIT53891.2022.9813965.

CHAPTER 3
FALSE DATA INJECTION MODELING AND DETECTION ON GPS DATA USING MACHINE LEARNING

3.1 False Data Injection Attack

This chapter models FDI attacks on GPS data gathered from a UAS environment. Specifically, timestamp data attributes were modeled as target parameters under multiple scenarios. The methods of multiple clustering techniques such as Density Based Spatial Clustering (DBSCAN), Ordering Points To Identify the Clustering Structure (OPTICS), Gaussian Mixture Models (GMM) and Hierarchical Clustering (HC) were also used for data processing purposes. Because UAS integration into national airspace is growing, it is more open to cybersecurity-related vulnerabilities.

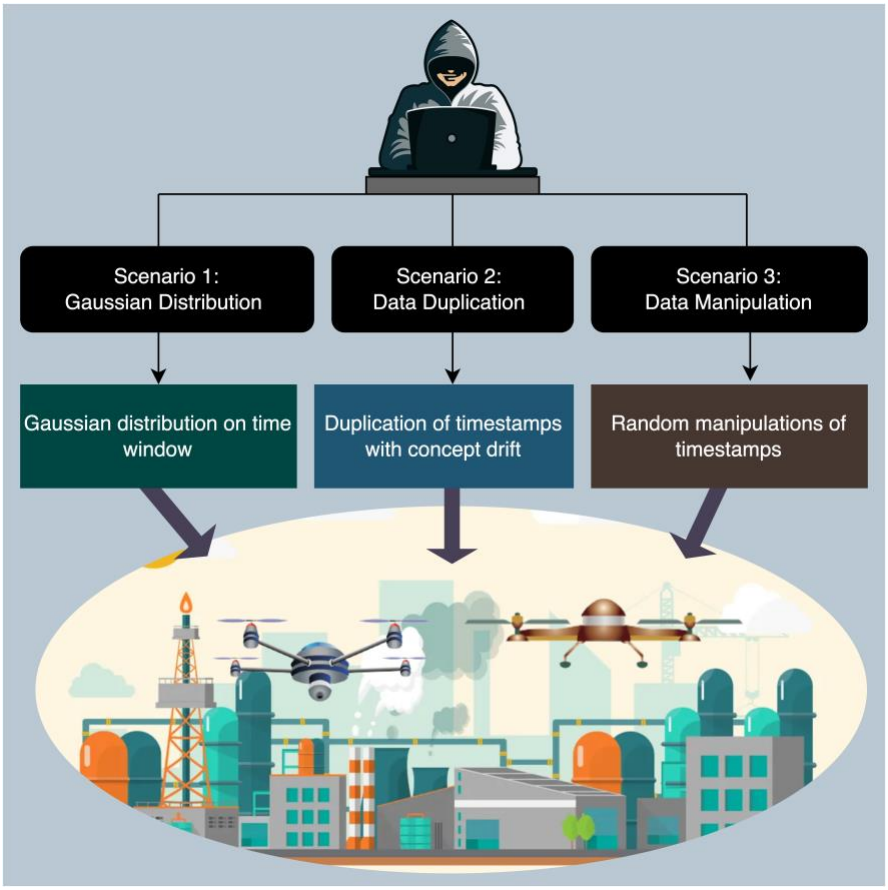


Fig. 6. GPS false data injection scenarios.

Cyber security attacks targeting GPS sensors within UAS may lead to incorrect timing, thus affecting sensing, communication, and control. This may lead to incorrect control responses in mission and trajectory planning, which is an uncertainty in situational awareness.

In this chapter we model three scenarios where GPS signals could be modified: 1) modeling FDI as the Gaussian Distribution; 2) manual data duplication of time stamps at different locations; and 3) random manipulation of time stamps. Fig 1. shows the false data injection scenarios in the UAS environment.

About the Dataset: In order to organize the dataset, a M300 UAS, which collected electric/magnetic field data at a 300kV power transmission line, was used. This dataset contains 4119 GPS messages in a time series. This data registered a total of 600-time stamp-related messages generated every minute, and a total of 4119 messages for a six-minute flight duration. Fig 7. shows the flight trajectory of the M300 drone at 345KV power transmission line.

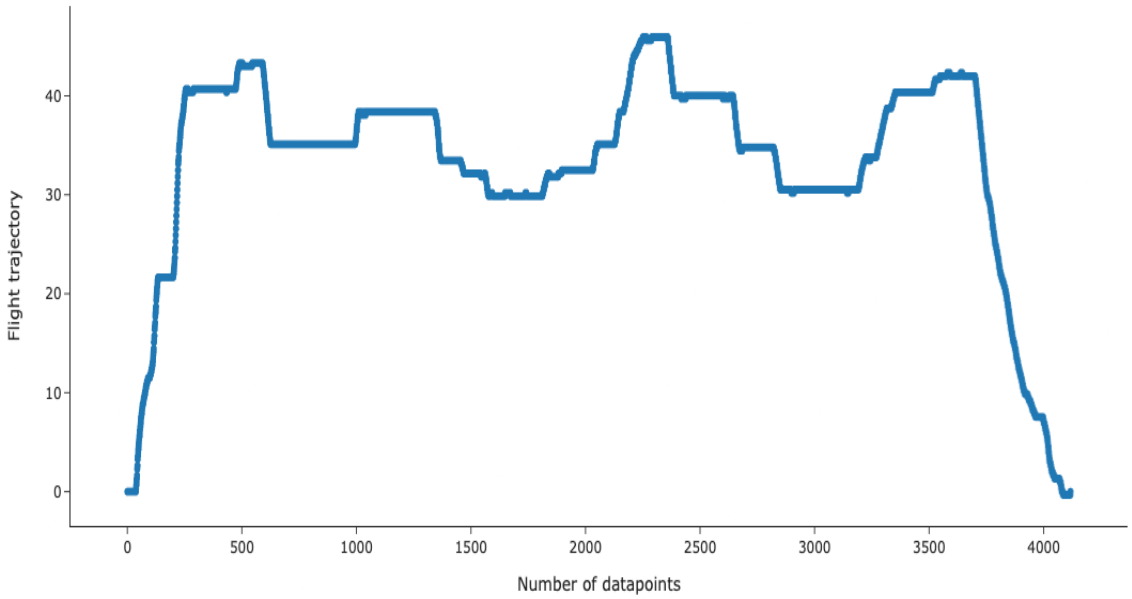


Fig.7. M300 flight trajectory at 345KV power transmission line.

3.2 Methodology

Scenario 1 is designed for noise injection where the GPS timestamps are considered for detecting noisy data or malicious activity. The Gaussian noise formula generates the noisy timestamps to manipulate the real GPS timestamps.

- **Scenario 1: Modeling FDI as Gaussian Noise Distribution (GND)**

In Scenario 1, FDI was modeled through GND. The following steps demonstrate the Scenario 1 flow.

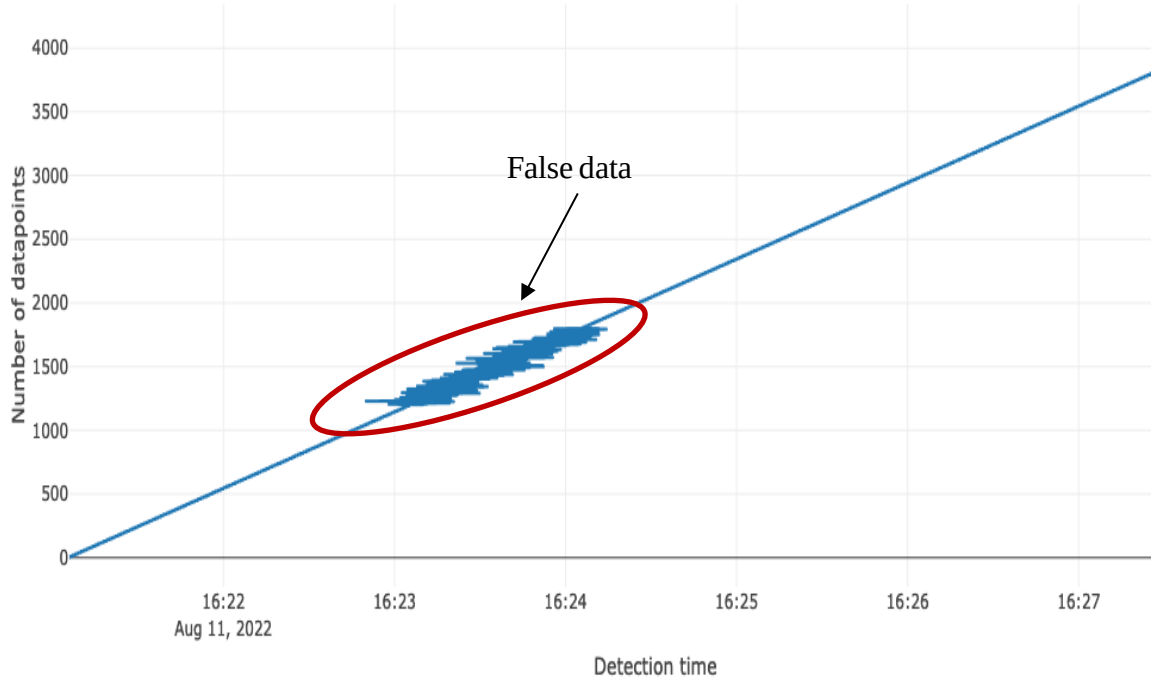


Fig. 8. Scenario 2: Data manipulation flowchart.

Step 1: Create a new feature column that will host FDI data.

Step 2: Select the time window for the attack execution on the flight data (i.e., 2 minutes).

Step 3: Generate fake time stamps for the time window that matches with average message frequency and length of the original flight. For example, a 2-minute window will generate 1200 messages.

Step 4: Apply the GDN on the timestamps, where f(t) is the noise in which mean and sigma is the variance of the distribution for timestamps.

$$f(t) = \mu + \sigma\varepsilon(t) \qquad (1)$$

Step 5: Merge the generated FDI data field with the original timestamps as seen in Fig 8 and the flow chart is shown in Fig 9.

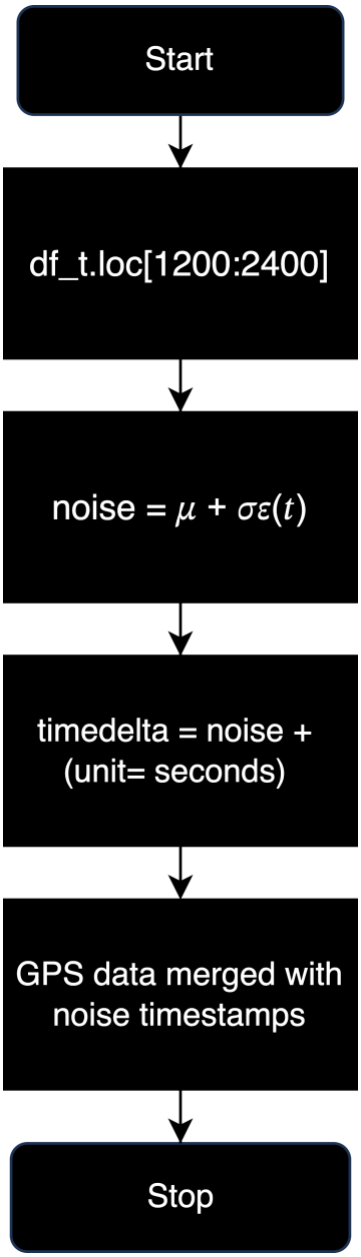


Fig. 9 . Scenario 3: Data manipulation flowchart.

- **Scenario 2: Data Duplication**

Scenario 2 models a duplication of the real-time stamps from GPS with varying seconds. Duplication of time stamps can occur due to clock skew, clock offset, or interference with the environment, payloads, and other sub-systems. It is important to catch these duplication of time fields (although rare) in a timely manner to avoid any integrity issues with GPS relied on systems or sensors.

Step 1: Choose an interval for duplication (2-min: 16:23-16:25), and type of duplication (i.e., 15 seconds delay to original timestamp).

Step 2: Remove 75% of original timestamps for the 2-min period, and replace with duplicated delay.

Step 3. Save the feature as a separate function, so this can be used randomly. Figs. 10 and 11 show the real timestamps altered with duplicate timestamps including the manipulation of 15 seconds.

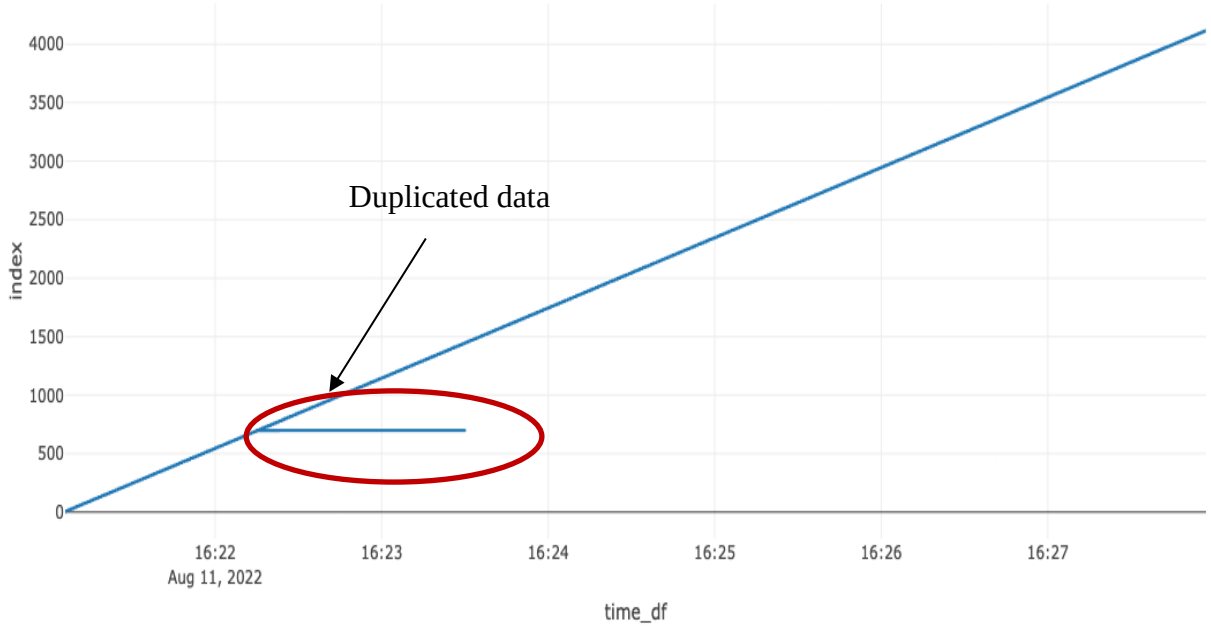


Fig. 10. Time stamps injection false data points

The flowchart of the data duplication is shown in the Fig. 11, where the main function of the injection uses 15 seconds of time delta function to increase the actual time for 15 seconds.

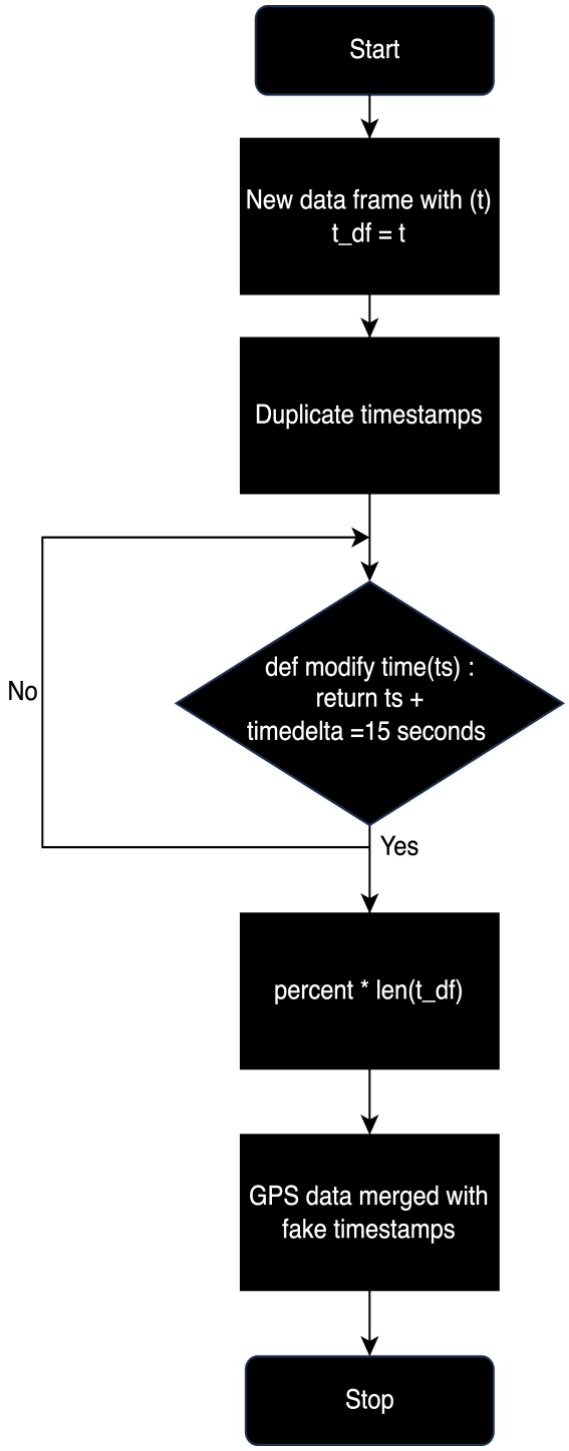


Fig. 11. Scenario 2: Data duplication for 2-minute time window.

- **Scenario 3: Data Manipulation**

Scenario 3 injects random duplication of timestamps with varying duration (0-30 seconds) to 75% of the data. The rate of 75% was determined and not increased further as the tested model was already not able to tolerate noise levels larger than 75%. Figs. 12 and 13 illustrate the random timestamp injection on real GPS timestamps.

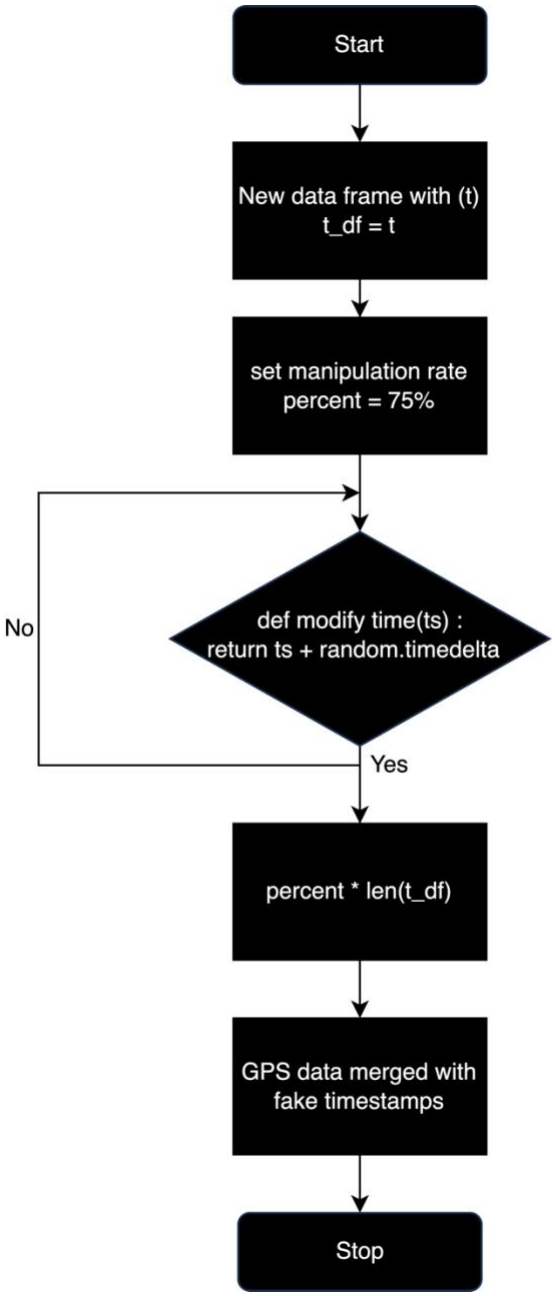


Fig. 12. Scenario 3: Random timestamp manipulation flowchart.

3.4 Clustering Methods for False Data Detection

- **DBSCAN**

DBSCAN clustering algorithm was selected to analyze the data points in this study as there is a wide deployment of this model to various applications containing noise. This method can be used for identifying anomalies in UAS. For instance, [15] reports that anomalies in flight phases such as take-off, pitch, and air density were detected by DBSCAN. [107] The same method was used with anomaly scores in risk and safety trends regarding the flight [108]. In [109], DBSCAN was also used to detect the outliers in the time series data. The model uses *eps* and *min_samples* as the components to form the data clusters. The number of min_samples for 'X' is set as 15 depending on dimension(d) + 1 core sample. The eps value =1 which results in 7 clusters for the data 'X'.

- **OPTICS**

OPTICS clustering algorithm [20] is close to DBSCAN. It groups the data points into clusters according to density. The density is determined by the reachability (ε) and minimum core (*min_samples*) values parameters [110]. In [111], the OPTICS clustering model was applied to the trajectory data that contains latitude, longitude, and altitude features to separate the clusters on the location information. The authors in [112] used OPTICS clustering for noise removal in LIDAR systems.

- **Gaussian Mixture Models**

Gaussian Mixture Model (GMM) is an unsupervised machine-learning model that uses probabilistic density functions for continuous measurements [113]. Since the GPS timestamps are linear and continuous in the air data, the GMM is applicable for clustering false data points for the related environment. In [114], the researchers used GMM for estimating the log-likelihood on a frame-level analysis so that replay and spoofing attacks can be detected.

Similarly, [23] used GMM for false data injection attack in smart grid applications. The GMM clustering algorithm uses *n_components* as a parameter that fixes the number of clusters assigned. For this data set, the optimal number of clusters for the data 'X' is 6 but it was set as *n_components* = 7 in the thesis to differentiate between normal and noisy data.

- **Hierarchical Clustering**

Hierarchial Clustering (HC) produces the output in the binary tree format as a *dendrogram*, which creates *nested data points* of different sizes. The bottom-up approach of hierarchical clustering has been referred as *agglomerative clustering*, which groups the data points into clusters based on the closest Euclidean distance. It has also been reported in several papers as a promising anomaly detection model. In [115], the authors used hierarchical clustering to cluster the time series data with the dynamic time warping (DTW) method.

We selected agglomerative clustering to separate the false timestamps into 7 different clusters to be compared with other models.

3.4 Metrics for Evaluation of Clustering

- **Silhouette Coefficient**

The silhouette coefficient (SC) evaluates the clustering by identifying the cluster compactness and separation of each cluster [116]. The parameter *a(i)* is calculated by the average distance to all other data points within the same cluster for each data point. *b(i)* refers to the average of all the data points in the nearest neighboring clustering for each data point.

The silhouette index for each data point is calculated using the formula:

$$silhouette(i) = (b(i) - a(i)) / max\{a(i), b(i)\} \quad (2)$$

The formula 2 calculates the overall silhouette index for the clustering analysis by taking the average of all silhouette values across all data points. A higher overall silhouette index (2 ıtes better clustering, where clusters are more distinct and well-separated. It is often used as a validation measure to assess the quality of clustering results and to determine the optimal number of clusters in unsupervised learning tasks. The purity of the cluster is evaluated based on the index ranges from -1 to 1 which states -1 being the least performed cluster and 1 being the well-performed cluster shown below[117].

$$-1 \leq s(d) \leq 1$$

Our analysis evaluated the SC for each cluster formed on the GPS timestamps.

- **Davies Bouldin Index**

Davies Bouldin Index is a quality metric for clustering algorithms, and it is identical to the silhouette coefficient metric. The centroid of the clusters is compared between the most similar and dissimilar clusters. The cluster diameter measured within the cluster is an inter-cluster similarity measurement and the measurement with another cluster is intra-cluster [118]. Davies-Bouldin Index for each cluster is calculated by using the following formula:

$$DBI(i) = (D(a) + D(b)) / d(a, b) \qquad (3)$$

D(a) is the average distance between all data points in cluster *a* and the centroid of cluster *a*. *D(b)* is the average distance between all data points in the neighboring cluster *b* and the centroid of cluster *b*. $d(a, b)$ is the distance between the centroids of cluster a and cluster b. The average distance measurements of both clusters are again averaged and then added up. The sum of the average distance is divided by the number of clusters formed. In terms of DBI score assessment, the lower DBI value refers to that higher quality where the clusters are well separated and distinct from each other. It also has small intra-cluster distances and larger inter-cluster distances.

DBI is applicable to the analysis of each cluster's performance based on the similarity of the data points and clusters formed. It is also essential to use the DBI accordingly as it could change based on the dataset and type of clustering problem at hand.

3.5 Conclusion

This chapter discussed false data injection modeling and its detection for GPS data sets. Four different clustering algorithms were deployed for multiple scenarios. Preliminary results indicate that OPTICS clustering suits timestamp duplication and random manipulation scenarios with mixed results and does not perform well for all scenarios. Quick deployment of the isolation forest model offered a better accuracy for scenarios 1 and 2 over clustering methods. Isolation Forest yielded an accuracy of 98% for the scenario 1, and 100% for the scenario 2. One-class SVM model resulted in the detection of maximum false data for the scenario 3. Further research is warranted to test its efficacy in streaming UAS data for FDI detection.

CHAPTER 4
GPS DROPOUT DETECTION AND RISK CLASSIFICATION ON UAS FLIGHTS

4.2 DJI Aeroscope and DFW UAS Flights

The DJI AeroScope was released in 2017 for drone detection and data recording purposes. It is a passive radio frequency sensor that detects the datalinks between remote pilot controls and UAS. The DJI Aeroscope sensor displays and captures the flight data from the aircraft. Within the electronic line of sight, the aeroscope receives telemetry of DJI UAS platform activity, by including information regarding the location of the unmanned vehicle, the position of the remote controller, the flight path, the altitude, the speed, the direction, and other parameters [119]. Generally, UAS are detected by the radio frequency communication data link that connects them to a remote controller for receiving control commands at 2.4GHz and aerial images. Detection and localization of the unmanned aerial vehicle are performed based on the spectral patterns of the aeroscope systems. Aeroscope systems are developed in two types stationary and portable. The stationary aeroscope covers a maximum 50 km range on large-scale sites and the portable aeroscope system is expected to cover a maximum 5 km range for temporary events and mobile deployment [120]. Fig. 14. is an image of a DJI Aeroscope with an antenna.

Fig. 13 DJI Aeroscope with G-16 antenna [123].

In this thesis work, GPS data was collected over 24 hours on 4th July 2021 for UASs in the range of a telemetry receiver located at the Dallas Fort Worth (DFW) Airport. The data was captured by a DJI Aeroscope G-16 antenna (stationary) model. The detection range of the drone is 20-30 miles with a 100-mile extension. The coverage criteria of 22.5-degree and the two frequency levels are 2400-2500 MHz and 5700-5850MHz; the power gain is 15.5 and 14 dBi. The dataset contains 18756 entries with 12 parameters. Detection Time (EDT), Drone ID, Flight ID, Latitude, Longitude, Speed, Altitude(m), Home Longitude, Home Latitude, Pilot Longitude, and Pilot Latitude are the parameters recorded by the DJI aeroscope. There are 536 drones with 22 drone types identified by the aeroscope sensor. Those drones made 1743 flights for surveillance purposes in a 24-hour period. The selected features for the analysis were Drone Type, Flight ID, Speed, Altitude, and Detection Time (EDT). Each feature was visualized and checked by the statistical measures and described in the subsections below. The Detection Time (EDT) was the most important feature for the time difference, outlier detection, and risk classification that was performed in this DJI aeroscrope dataset analysis. This analysis decision was made on the message frequency and time difference findings.

4.3 Drone Types and Flights

Threats may occur from a single drone or a group of drones, but the identification of drone type is important for safety and security [121]. In [122], the authors performed drone-type detection through machine learning models. The drone type was labeled according to the value of a particular drone characteristic, such as the payload or the number of rotors, as in the context of a drone characterization and categorization process. There were 22 drone types detected by the DJI aeroscope sensor. The types included one unknown drone type. The drone types were FPV, M200 V2, M300 RTK, Mavic 2, Mavic 2 Enterprise Advanced, Mavic Air 2, Mavic Air 2 Mini, Mavic Air 2 S, Mavic Mini 2, Mavic Air, Mavic Mini, Mavic Pro, P3 series, P3P, P3S, P3SE, P4, P4

RTK, P4P Series, P4P 2.0, Spark and unknown drone type. Several flights were made by different drone types at the DFW airport. Fig.15. shows the drone types of all the flights and message counts on the ‘y’ axis.

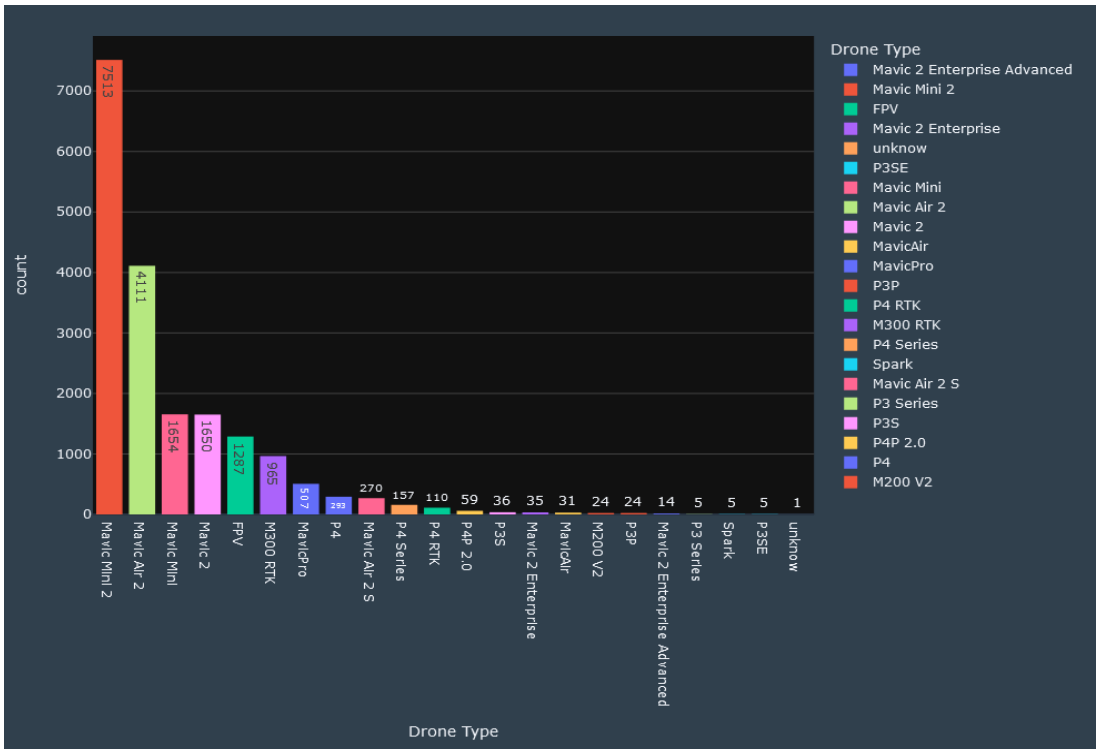


Fig.15. Number of messages collected by different drone types.

The number of flights was 18756 with 22 drone types made in the dataset. Table 4 illustrates the top 3 drone types, and their time difference in seconds.

Table 4. Time difference of the drone types (with data points).

Drone Type	Mean (s)	Median (s)	Mode (s)
Mavic Mini	48	3	2
Mavic Air	18	2	0
Mavic Mini 2	11	1	0

The records stated Mavic Mini had 2 seconds time difference frequently proven from mode results. The message frequency of Mavic Air and Mavic Mini looked normal based on the

mode values. The detailed analysis of time difference, drone type, and message frequency is discussed in the statistical technique results in upcoming parts of this thesis content.

4.4 Drone Speed

The drone speed impacts the drone range, energy consumption, and battery life [123]. Fig 16. shows the speed of different drone types. It shows that drone types FPV, Mavic, and Mavic Air 2 have the fastest speed compared to other drone types.

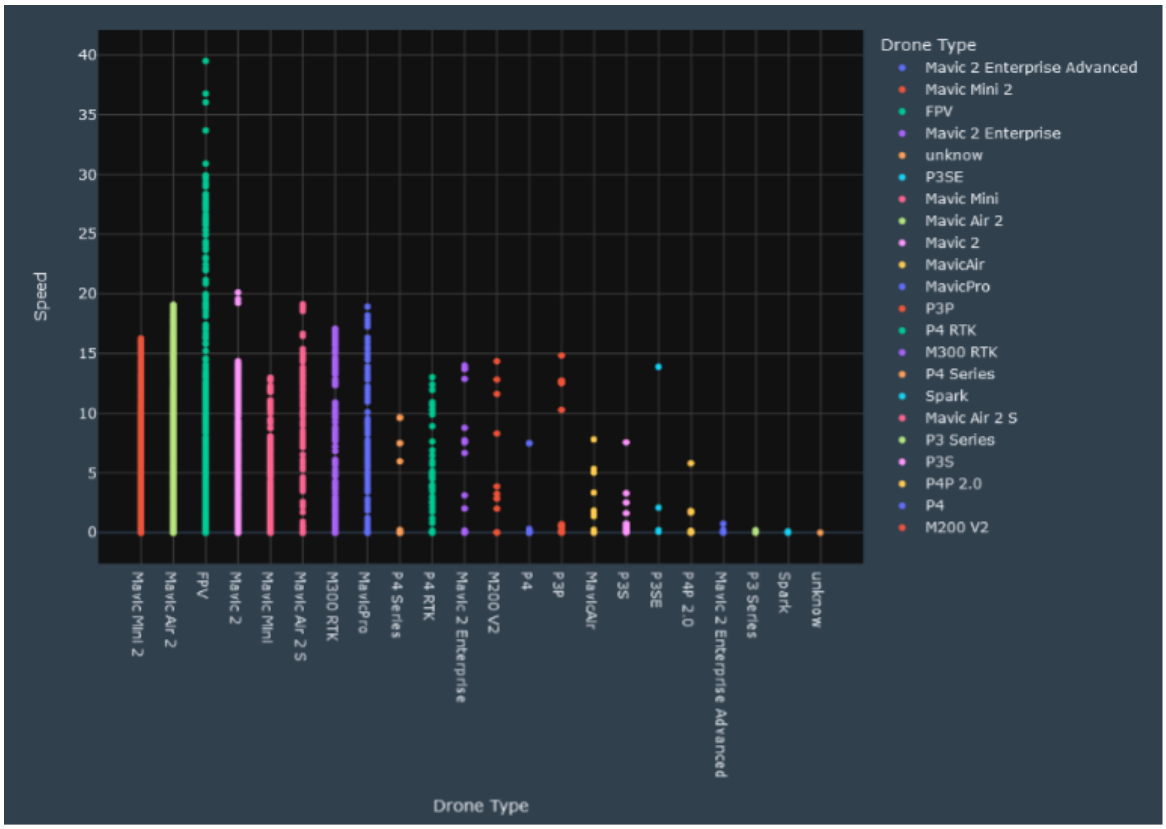


Fig14. Drone speed of all the flights.

4.5. Drone detection time and time estimation

Detection time is the main feature of the dataset that allowed the computation of GPS dropout through message reporting frequency. The detection time feature allows monitoring of the duration as well as messages from UAS flights. The difference in detection time between one message and the next message is considered as the time difference.

Fig. 17 is the histogram of time difference on each drone type. Mavic Mini 2 and Mavic Air 2 are the two types of drones with the longest recorded time difference.

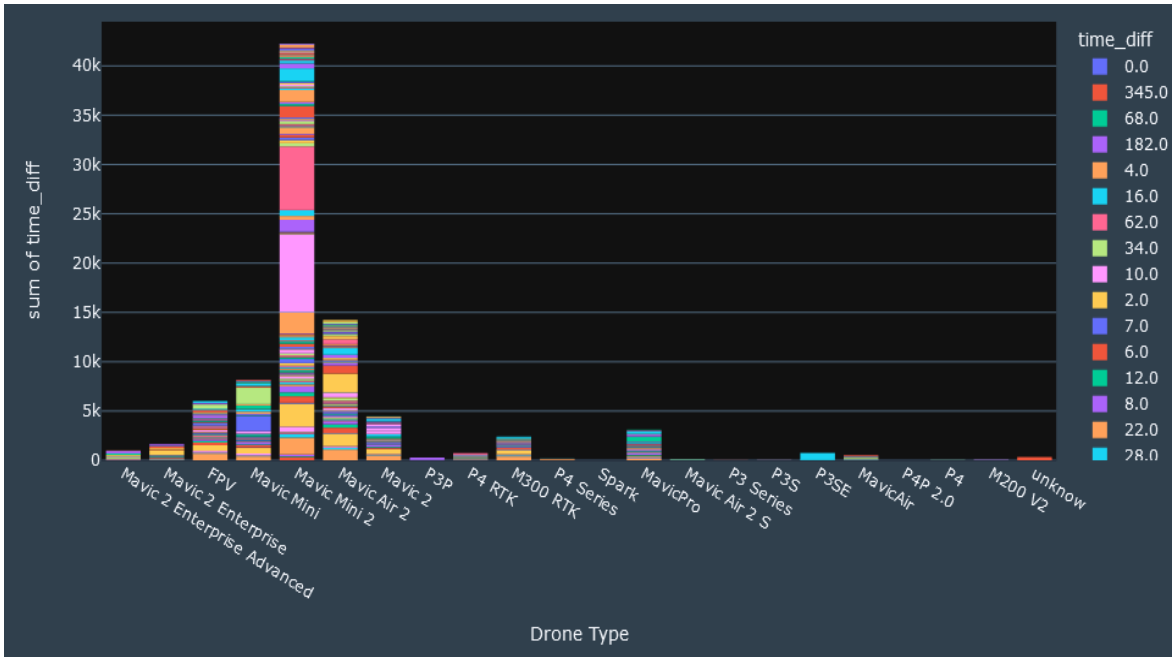


Fig 15. Drone detection time and its time difference.

Among several flights recorded in the dataset, Flight ID 625 contained the largest number of messages got from the receiver. Fig. 18 is the 3-Dimensional (3D) view of time difference with altitude and detection time features.

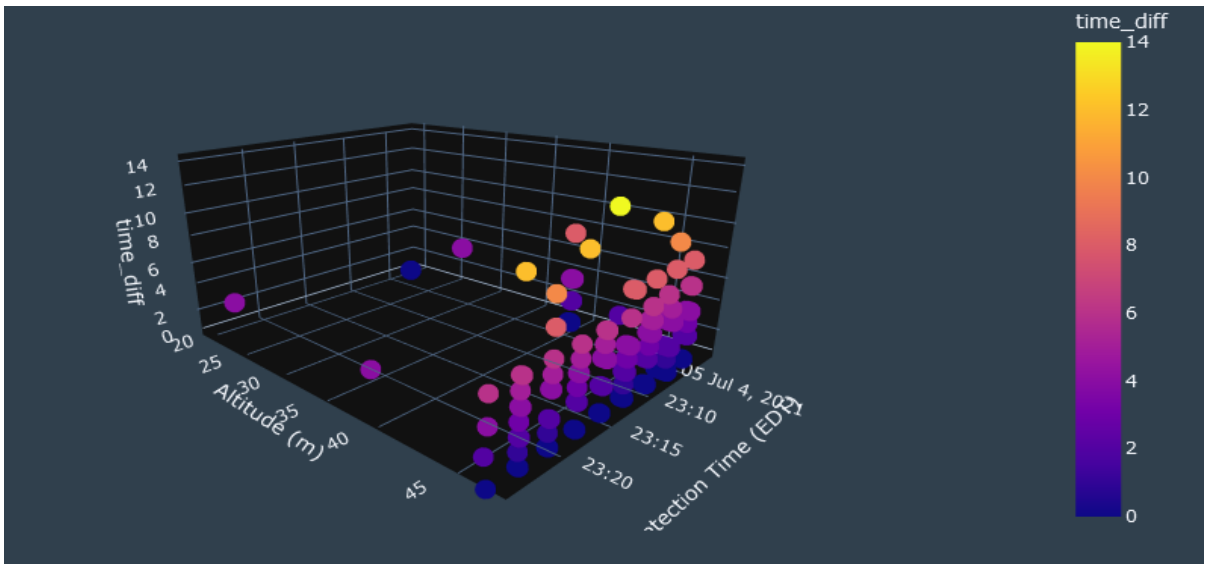


Fig 16. Time difference of the flights at altitude.

It is important to check the altitude level of the longest-time difference to mitigate the probability of dropout at a particular altitude level. Based on the analysis, it is seen that more than 10 seconds of dropout was detected at an altitude above 350 ft. Table 5 shows the summary time difference values of different time windows.

Table 5. Summary of time difference in different time windows.

Time difference window	No. of Flights	No. of Drones	Average Altitude (m) of Time difference range
1s- 3s	669	100	107
3s-5s	127	43	83.54
6s-10s	70	30	68.37
>10s	1338	352	113.93

4.6. ADS-B/GPS Dropout Detection on UAS Flights in Alaska

GPS dropout of the flight is estimated by computing and tracking the time difference between consecutive messages. Seven flight (Mavic Air 2) datasets were provided by the Research Institute of Autonomous Systems (RIAS) at the University of North Dakota. This dataset was utilized to compare the message frequency of aeroscope sensor data and DJI air data.

Dataset Information

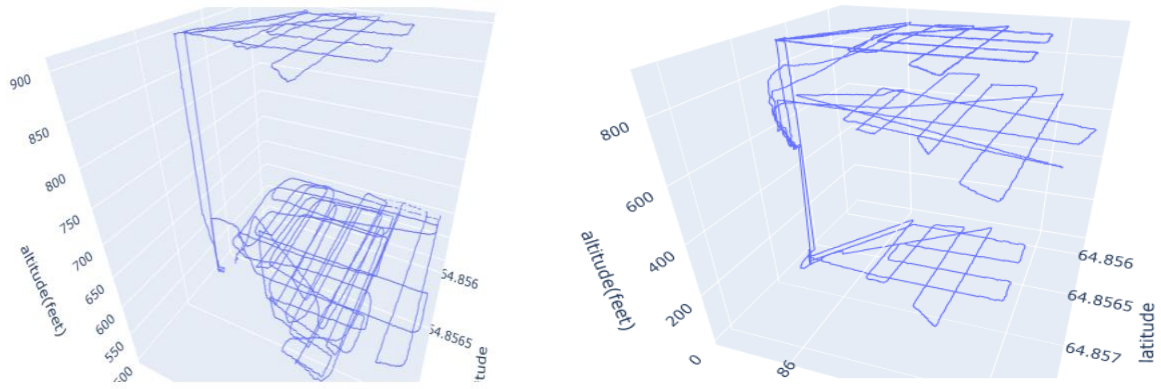
The UAS flights in Alaska contained two dates: Feb 21, 2022 and Feb 23, 2022. Table 4 represents actual flight parameters. Also, Table 6 shows flight parameters captured by Mavic Air 2 in Alaska.

Table 6. Flight parameters captured by Mavic Air 2 in Alaska.

Date	Origin Time	End Time	Flight Duration	No. of Entries
02/21/2022	18:16:00	18:26:07	0:09:50	4498
	19:15:38	19:24:18	0:08:40	3967
	20:07:00	20:16:00	0:09:00	4005
	23:04:58	23:14:06	0:10:00	4146
02/23/2022	18:25:41	18:35:04	0:09:19	4288
	20:20:08	20:33:18	0:13:10	5983
	21:36:44	21:54:34	0:17:50	8082

4.7 Flight Trajectory and Time Difference

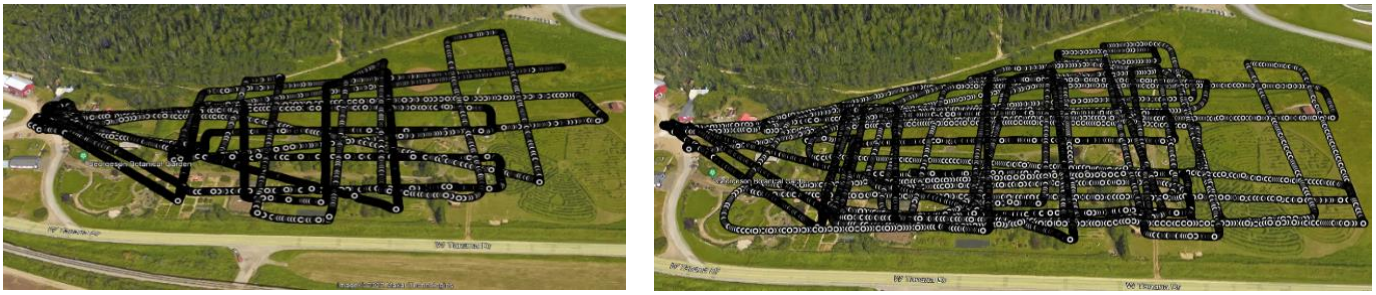
The data set contained four flight trips for Feb 21, 2022, and three ones for Feb 23, with a total of 7 flights. The trajectory of all the flights for each day is shown in a 3D view in the context of Fig. 19 (a) and 19 (b).



(a) (b)

Fig 17. Flight trajectory of (a) 21st February 2022, and (b) 23rd February 2022.

It is observed that (See Figs 20 (a) and 20 (b)), there were no missing data on latitude, longitude, and altitude information, according to the trajectory plots.



(a) (b)

Fig 18. Flight trajectory in Google in Earth (a) 21st February, and (b) 23rd February 2022.

To develop criteria for dropout rates, it is important to capture actual message reporting frequency. Thus, each flight was analyzed in multiple rolling windows. Table 7 shows message frequency and rolling mean summary of the Alaska flights dataset.

Table 7 Rolling Mean of message frequency by time window.

Date	**Flight**	**Flight Duration**	**Overall Mean**	**Rolling Mean every 1-minute interval: [mean, # of messages]**		**Rolling Mean every 2-minute interval: [mean, # of messages]**		**Rolling Mean every 3-minute interval: [mean, # of messages]**		**Total No of Messages**
02/21 /2022	1	0:09:50	0.1318	0.131151	408	0.131149	749	0.131133	1124	4498
	2	0:08:40	0.1311	0.131240	396	0.131264	661	0.131263	991	3967
	3	0:09:00	0.13119	0.134865	400	0.134898	667	0.134932	1001	4005
	4	0:10:00	0.14475	0.144962	376	0.138922	691	0.136277	1036	4146
Aggregate Statistics				0.135554	395	0.134058	692	0.133401	1038	4154
02/22 /2022	1	0:09:19	0.1313	0.131210	389	0.131217	714	0.131212	1072	4288
	2	0:13:10	0.13206	0.132075	427	0.132070	854	0.132077	997	5983
	3	0:17:50	0.132409	0.132383	461	0.132384	801	0.132386	1154	8082
Aggregate Statistics				0.131889	425	0.131890	790	0.131891	1074	6117
Overall Aggregate of all the flights				Mean of time difference - 0.133502				Average no. of messages reported - 6462		

This data was very small to arrive at meaningful inference, but it seems there were no dropouts or at least this drone contained very frequent message reporting every minute.

4.8 Risk Labeling

Based on the message frequency analysis and outlier detection, the length of the time difference in different ranges was labeled. In Table 2, the time difference range was categorized and assigned to an encoding.

Table 8. Risk label of time difference category.

GPS Dropout Impact Level		
Time Difference	**Risk Level**	**Risk label Encode**
0	No Dropout	0
1s to 2s	Low	1
3s to 5s	Medium	2
6s to 10s	High	3
Above 10s	Lost	4

The categorization was made to measure the impact level of GPS dropout on UAS flights. The dataset and message reporting frequency analysis of the research indicate low and medium dropout with the maximum number of flights at DFW airport.

Fig.21. The dropout category of all the flights with time difference ranges. The ‘x-axis in the figure is the risk level labeled for various time difference categories and the ‘y’ axis is the count of the messages received for all the flights of different drone types.

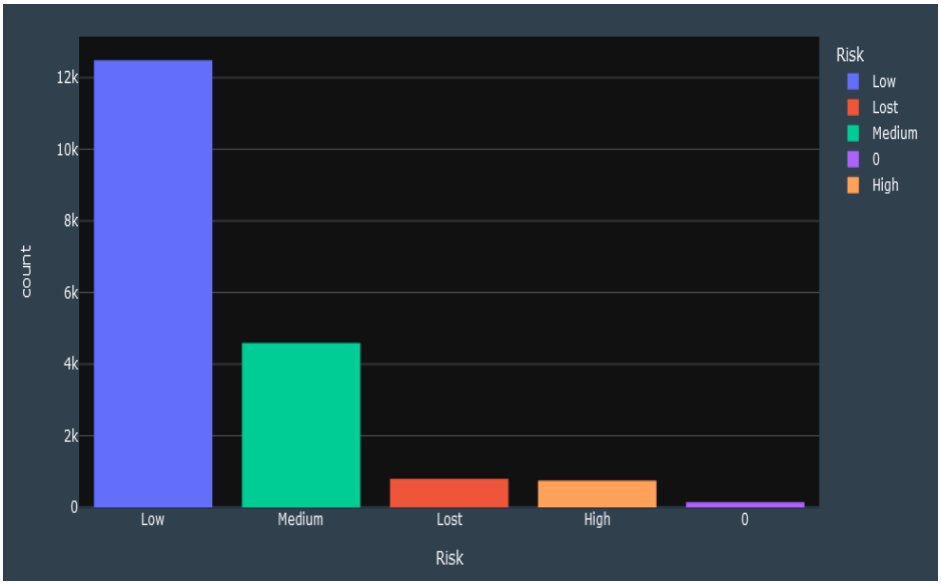


Fig. 19. Time difference category of all flights.

4.9 Evaluation Metrics for Risk classification

Evaluation metrics used for risk classification were confusion matrix, Precision, Recall, F1 Score, and accuracy [124]. In this analysis, we used Precision, Recall, F1 score, Support and Accuracy to understand the model performance. The parameters for Precision and Recall are True Positives (TP) and False Positives (FP) and False Negatives (FN). Precision ensures the reliability of the model by the number of TP rate. Here, Precision, Recall, F1 score, Support and Accuracy were used to understand the model performance. The formula for Precision and Recall parameters are True Positives (TP) and False Positives (FP) and False Negatives (FN). Precision ensures the reliability of the model by the number of TP rate.

$$Precision = \frac{TP}{TP + FP}$$

Recall defines the predictive accuracy of the TP values in a model and indicates the potential of the model to find the TPs successfully.

$$Recall = \frac{TP}{TP + FN}$$

F1 score is the harmonic mean of precision and recall and it is also a tradeoff between those two quantities. The maximum value of the F1 score is 1 and the minimum is 0, as refering to the model performance from precision and recall.

$$F1 - Score = \left(\frac{2}{precision^{-1} + recall^{-1}}\right) = 2\left(\frac{precision.recall}{precision + recall}\right)$$

Support is the metric that sums up the true positives and false negatives of each class in the classification model.

$$Support = TP + FN$$

Accuracy is the overall model performance metric of the classification algorithm and accounts for the sum of TP and TN and the division of precision and recall denominator.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

F1-Score and Accuracy are two metrics that evaluates risk level class of each algorithm. We used multiple supervised machine models to classify the impact of the dropout length of all the flights. The Machine learning models used in the classification have been *Random Forest, Support Vector Machine, Decision Tree, Logistic Regression, and Naïve Bayes. Sequential Neural Network* and *Multi-layer perceptron* are the feedforward neural network models that we experimented in this analysis.

CHAPTER 5
RESULTS AND DISCUSSION

The results of GPS anomaly detection based on FDI attack modeling and GPS dropout risk classification model reports are shown in this chapter. FDI scenarios are detected with clustering and outlier detection algorithms. The clustering algorithms formed a cluster of data points and resulted in a different set of clusters for each scenario. There are 7 clusters that were formed by DBSCAN and OPTICS. To compare the cluster performance with DBSCAN technique, the *n_components* = 7 is set to match the number of clusters for the GMM and the HC. The clustering models were evaluated by two indices: Silhouette Coefficient and David Bouldin's Index. A large value in the Silhouette score is considered a good grouping while a low value indicates an outlier. For example, the silhouette scores are negative (-0.63 for scenario 1; -0.79 for the scenario 2; and positive lower value for the scenario 3). Both DBSCAN and OPTICS performed well for the scenario 1, as negative values were reported in several clusters. GMM and HC do not perform well, if we consider the Silhouette scores obtained for these scenarios. Also, OPTICS combined both normal and outlier points in the scenario 1, indicating that it is unable to distinguish the difference between them, as pointing a serious concern. OPTICS performed better for the scenario 3 than other scenarios. If we consider DB scores comparing all methods, then both DBSCAN and OPTICS yield larger positive values over other methods. Specifically, DBSCAN yielded a DB value of 2.883, and OPTICS showed 2.77 indicating good performance. However, as all clusters contained same DB scores, distinguishing outliers is a challenge for using DB index. Thus, while evaluating DBSCAN and OPTICS for all scenarios, it was better to distinguish the clusters by using SC scores rather than DB index. With DB index, OPTICS yielded 2.56 for scenario 2. It was larger when compared to other methods, but still faced the issue of distinguishing clusters. GMM yielded DB of 0.49, which is a lower value compared to

other methods. However, it yet faced the problem of distinguishing specific clusters. Table 9 shows the parameters and its values for OPTICS clustering.

Table 9 Parameters for OPTICS clustering.

Scenario	OPTICS Parameters		
	min_samples	*max_eps*	*metric*
1	35	1.5	minkowski
2	20	1.5	minkowski
3	15	1.5	minkowski

5.2 Clustering Outlier Detection

Figs. 22, 23, and 24 show the results for DBSCAN and OPTICS clustering algorithms, considering all three scenarios. The obtained findings are shown in Table 2. HC and GMM performed poorly so the results were not represented.

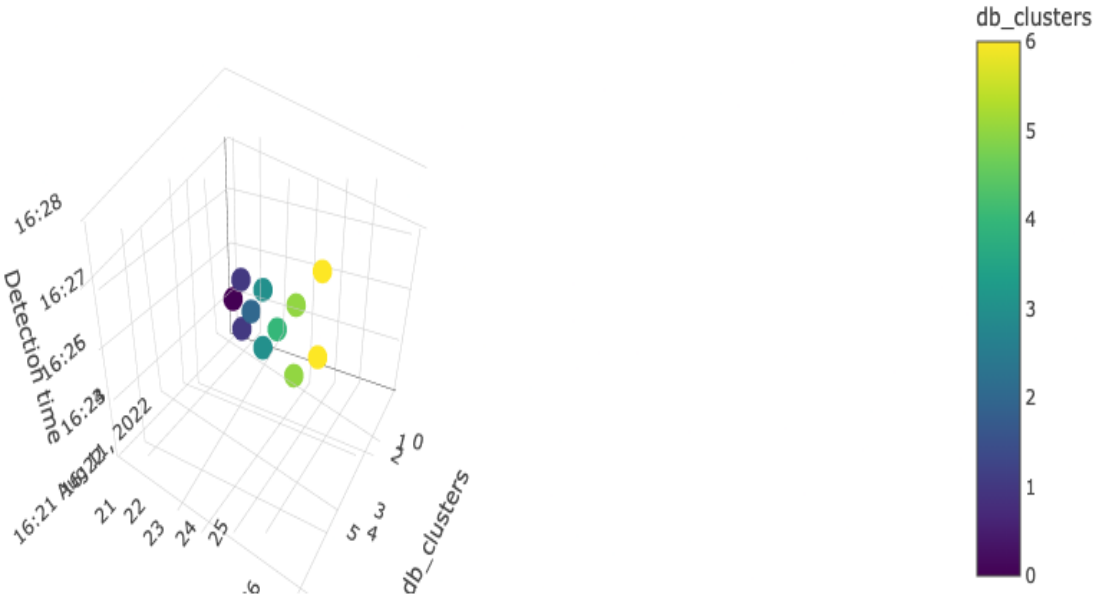


Fig. 20 DBSCAN clustering output for the scenario 1.

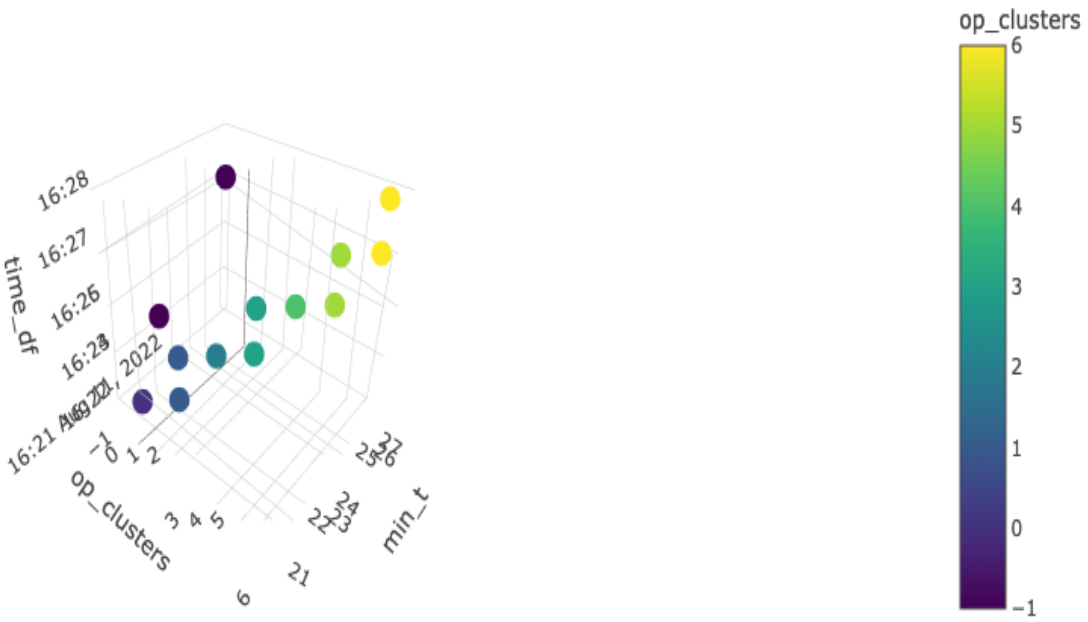


Fig. 21 OPTICS clustering output for the scenario 2.

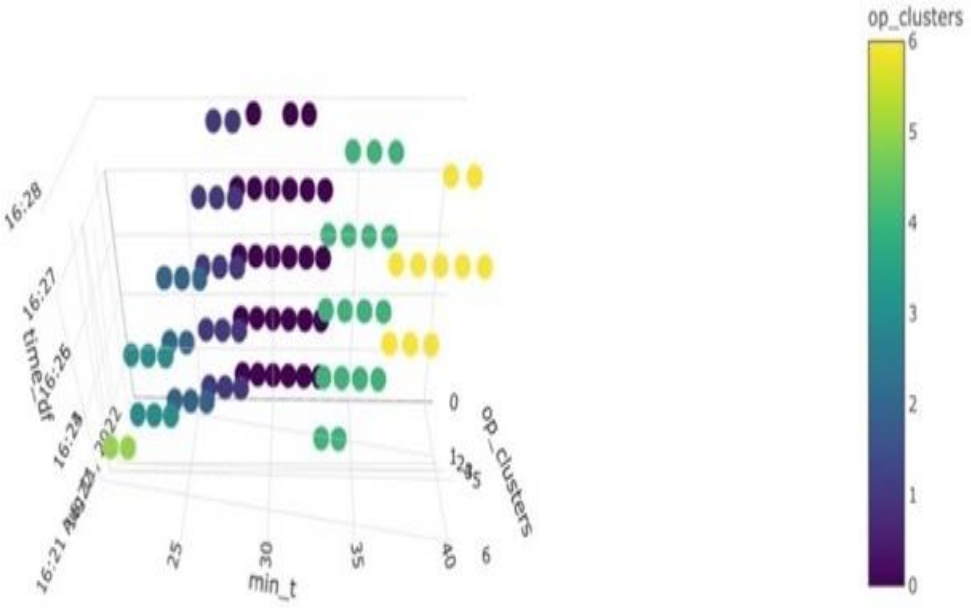


Fig. 22 OPTICS clustering output for the scenario 3.

Table 10. Clustering results for the used metrics.

Model	Cluster	Data points			Silhouette Coefficient			Davies Bouldin Index		
		Reported number of clusters out of 4119 total points with 1200 injected points (scenarios 1-2), 1030 injected points (scenario 3)			*Scenario 1*	*Scenario 2*	*Scenario 3*	*Scenario 1*	*Scenario 2*	*Scenario 3*
DBSCAN	0	1283	540	540	0.30	0.59	0.64	2.883387	0.44596	0.436441
	1	270	600	601	0.32	0.49	0.53			
	2	87	600	599	0.69	0.57	0.50			
	3	651	600	600	-0.17	0.58	0.51			
	4	36	600	600	-0.08	0.57	0.68			
	5	40	601	601	-0.23	0.62	0.55			
	6	1746	578	578	-0.24	0.72	0.54			
	-1	6	-	-	1.00	-	-			
OPTICS	0	35	540	420	0.84	0.59	0.64	2.711280	2.560939	0.432661
	1	41	600	469	0.00	0.49	0.53			
	2	53	591	509	0.00	0.59	0.50			
	3	71	600	475	-0.30	0.58	0.51			
	4	34	600	480	0.84	0.57	0.68			
	5	59	601	466	0.38	0.62	0.55			
	6	58	569	497	0.84	0.79	0.54			
	-1	3657	18	803	-0.63	-0.79	0.23			
Gaussian mixture models	0	608	600	600	0.48	0.57	0.50	0.383004	0.44459	0.494558
	1	616	600	601	0.51	0.49	0.50			
	2	587	578	578	0.67	0.78	0.68			
	3	594	600	599	0.54	0.57	0.56			
	4	591	600	600	0.53	0.58	0.53			
	5	536	540	540	0.65	0.59	0.64			
	6	587	601	601	0.53	0.62	0.53			
Hierarchical Clustering	0	758	760	760	0.40	0.57	0.57	0.362125	0.48892	0.434902
	1	724	689	689	0.40	0.49	0.49			
	2	563	659	659	0.52	0.78	0.78			
	3	588	630	630	0.50	0.57	0.57			
	4	572	500	500	0.73	0.58	0.58			
	5	499	492	492	0.63	0.59	0.59			
	6	415	389	389	0.66	0.62	0.62			

5.2 Non clustering Outlier Detection

- Due to the lower accuracy observed in clustering methods, we investigated methods such as Isolation Forest, Local Outlier Factor, and One-class SVM models for this data set.
- We did not introduce evaluation metrics for the models as no test and train split criteria are applicable for this detection process.
- In [125], the authors explained how these outlier detection models detect false data injection attacks. Table 3 show its performance for three scenarios.

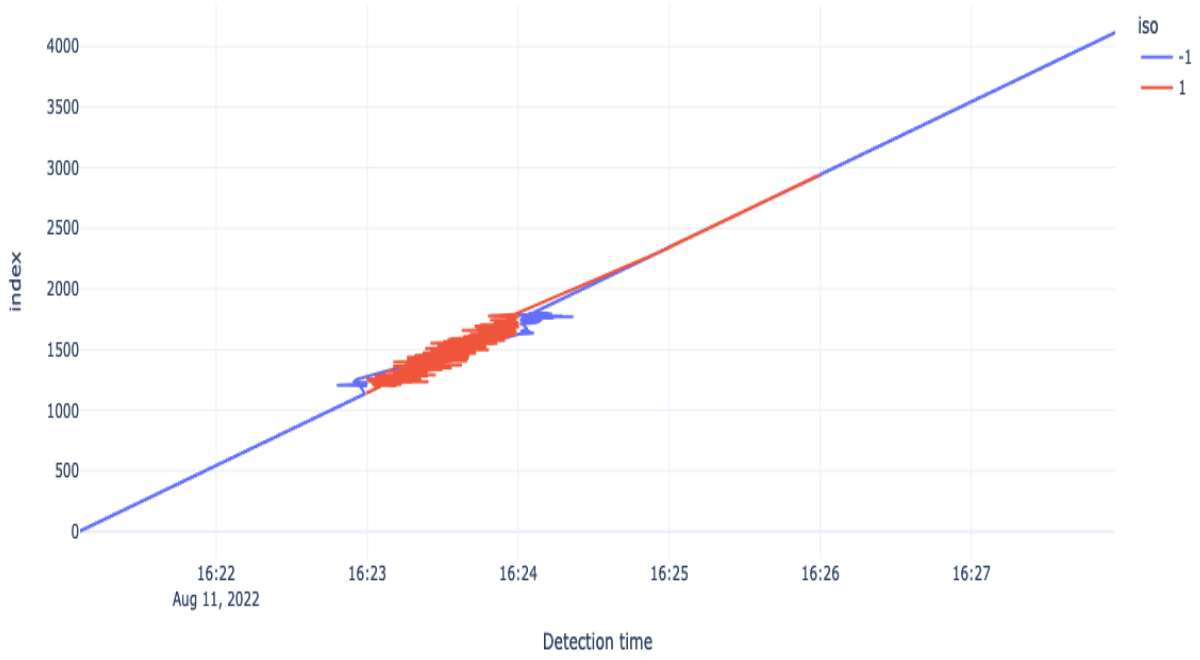


Fig.23. False data injection detected by Isolation Forest model in the scenario 1.

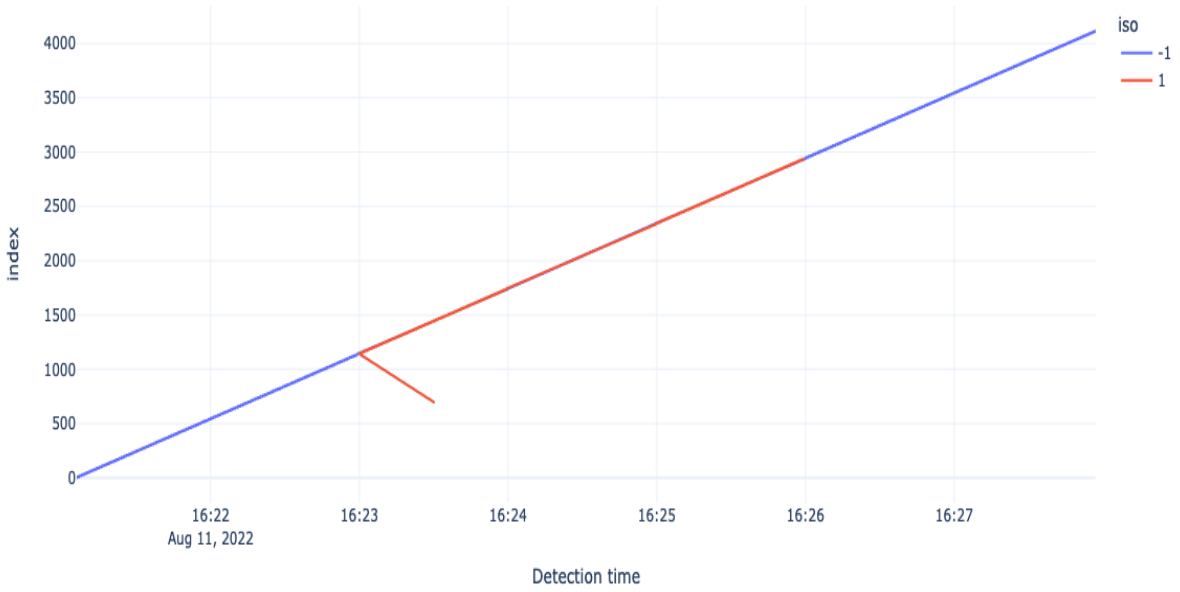


Fig 24. False data injection detected by Isolation Forest model in the scenario 2.

Table 11. Non-clustering model results.

Model	**Detected datapoints/ Injected data points**		
	Scenario 1	***Scenario 2***	***Scenario 3***
Isolation forest	1187/1200	1200/1200	1810/3088
Local Outlier Factor	787/1200	682/1200	268/3088
One-class SVM	0/1200	1958/1200	1959/3088

From the results in Table 11, it is evident that the isolation forest model proves to have the potential to detect the false data produced by the Gaussian distribution method and data duplication methods in scenarios 1, and 2. However, the same model included real data for the detection process in the scenario 3. The local outlier factor detected false data up to 50% of the

amount of injected data points. Figures 11 and 12 show the injected data detection on the isolation forest model.

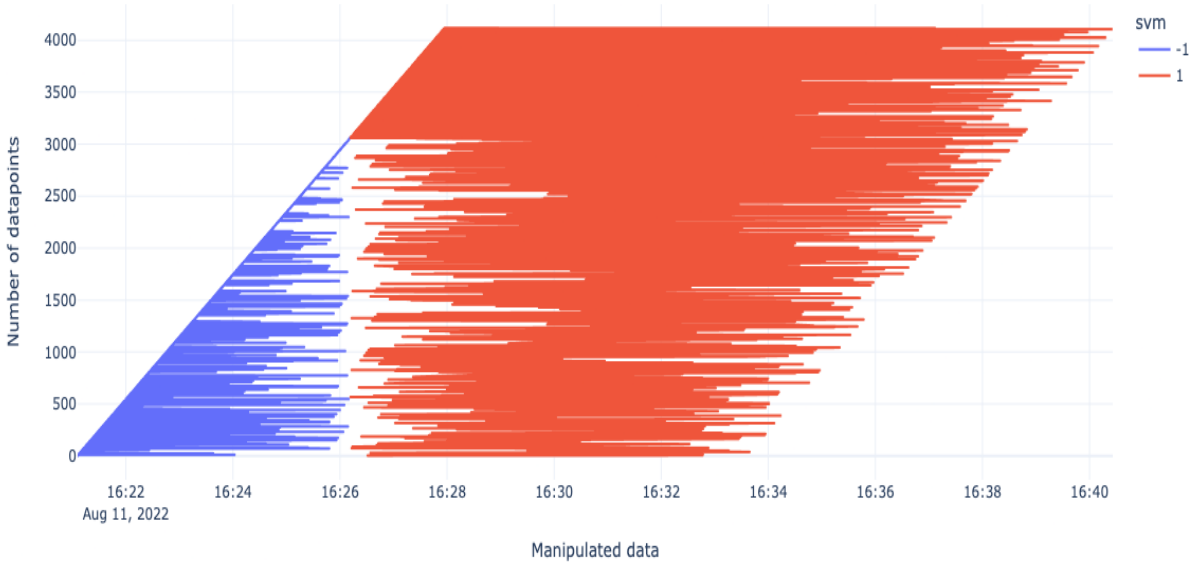


Fig 25. One-Class SVM model output for Scenario3

5.3 Multiclass Classification

A classification model that identifies the probability of each data point by assigning it to a specific class for prediction. Binary classification of two classes is the most common method for a classification problem in supervised machine learning. It assigns the data point to a class with the highest probability. If a classification problem involves more than one class for classification and prediction of probability, then it is called as multi-class classification. The performance of a classification model is evaluated via multiple metrics. Multi-class classifier evaluation compares the performance of many models and aligns the behavior of one class with hyperparameter tuning. The performance of the model uses the standard metrics with the method as a performance indicator.

Table 12. Multi-classification report of the models.

Random Forest	**index**	**precision**	**recall**	**f1-score**	**support**
	no dropout	0.00	0.00	0.00	34
	high	0.00	0.00	0.00	136
	lost	0.00	0.00	0.00	148
	low	0.89	1.00	0.94	2506
	medium	1.00	1.00	1.00	928
	accuracy		0.92		
Support Vector Machine	index	precision	recall	f1-score	support
	no dropout	0.00	0.00	0.00	36
	high	0.00	0.00	0.00	218
	lost	0.00	0.00	0.00	236
	low	0.79	0.96	0.86	3745
	medium	0.49	0.38	0.43	1392
	accuracy		0.73		
Decision Tree	index	precision	recall	f1-score	support
	no dropout	0.00	0.00	0.00	44
	high	0.00	0.00	0.00	220
	lost	0.00	0.00	0.00	230
	low	0.88	1.00	0.94	3734
	medium	1.00	1.00	1.00	1399
	accuracy		0.92		
Logistic Regression	index	precision	recall	f1-score	support
	no dropout	0.00	0.00	0.00	44
	high	0.16	0.04	0.06	220
	lost	0.42	0.04	0.08	230
	low	0.70	0.99	0.82	3734
	medium	0.42	0.07	0.12	1399
	accuracy		0.67		
Naïve Bayes	index	precision	recall	f1-score	support
	no dropout	1.00	0.89	0.94	44
	high	0.49	1.00	0.65	220
	lost	0.05	0.00	0.01	230
	low	0.90	0.97	0.93	3734

	medium	0.90	0.71	0.79	1399
	accuracy		0.86		
Sequential Neural Network	index	precision	recall	f1-score	support
	no dropout	0.00	0.00	0.00	0
	low	0.92	0.81	0.86	2812
	medium	0.47	0.52	0.49	853
	high	0.89	0.00	0.00	0
	lost	0.31	0.59	0.41	87
	accuracy		0.74		
Multi-Layer Perceptron	index	precision	recall	f1-score	support
	no dropout	0.00	0.00	0.00	0
	low	0.00	0.00	0.86	2794
	medium	0.00	0.00	0.50	957
	high	0.79	0.96	0.00	0
	lost	0.49	0.38	0.43	91
	accuracy		0.73		

5.4 Conclusion

One-class SVM failed in the scenario 1 and ensures no significant results for the scenario 2. However, it covered the false data manipulated inside the dataset for the scenario 3. Figures 11, 12, and 13 represent different scenarios showing injected data. The related results belong to false data injection modeling and the detection for GPS data sets. Four different clustering algorithms were deployed for multiple scenarios. Preliminary results indicated that OPTICS clustering suits timestamp duplication and random manipulation scenarios with mixed results and does not perform well for all scenarios. Quick deployment of the isolation forest model offered a better accuracy for scenarios 1 and 2 over clustering methods. Isolation Forest yielded an accuracy of 98% for the scenario 1, and 100% for the scenario 2. One-class SVM model maximum false data for the scenario 3. Further research is required to test the efficacy in streaming UAS data for FDI

detection. Dallas Fort Worth Airport UAS surveillance dataset was analyzed with statistical functions and machine learning models to identify the risk level of the GPS dropout. The study and research methods influence the messages received from the multiple drone types and flights. The outliers are the indicators for the GPS dropout detection and the classification models are the methods to categorize the impact of risk. This work supported our research for ADS-B and GPS dropout detection and mitigation on UAS flights for safety applications. Future work involves the detection and classification of dropout type to identify intentional and non-intentional interference that caused GPS dropout in the flight trajectory. This criterion provided flights with enough data to perform statistical analysis on the time delay between consecutive messages of unique flights, while flights containing fewer messages were discarded for major message frequency analysis.

5.5 Main Contributions

The contributions of the thesis are as follows:

1. Conducted a review of 5G cyber threats for 5G networks.

The first contribution provides a review of potential cybersecurity threats on 5G networks. The review categorizes the cyber-attacks on 5G networks into the major services of 5G, such as eMBB, mMTC, and URLLC. The risks and consequences associated with cyber-attacks were identified for different types of attacks on the Physical, Local, and Remote levels of the network. Preventive measures and mitigation strategies were also recommended for potential cyber-attacks.

2. Modeled and Detected a False Data Injection Attack.

The second contribution is about modeling a specific cybersecurity attack, i.e., FDI, to detect anomalies in GPS timestamps of UAS data. FDI attacks were modeled in three different

scenarios, such as Gaussian noise injection, data duplication, and data manipulation. Multiple clustering algorithms and outlier detection algorithms were introduced for the detection of FDI attacks in UAS data.

3. Classified a risk level for GPS dropout of multiple drone types.

The risk level needs to be determined for any GPS dropout that happens in the UAS navigation. Statistics of the time difference in GPS timestamps captured by DJI aeroscope were shown and the risk level was predicted by the multi-class classification models to identify the risk level of the GPS dropouts in the UAS environments.

The contributions were published in the following conferences.

- **Mohan, Jaya Preethi**, Niroop Sugunaraj, and Prakash Ranganathan. "Cyber Security Threats for 5G Networks." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 446-454. IEEE, 2022.
- **Mohan, Jaya Preethi**, and Prakash Ranganathan. " GPS False Data Injection Modeling and Detection using Machine Learning." In 2023 The 21st International Conference on Embedded Systems, Cyber-physical Systems, Applications (ESCS'23: July 24-27, 2023; Las Vegas, USA).

The codebase for the GPS anomaly detection and risk classification on UAS environments is updated on the https://github.com/Jayapreethi/gps_codebase.git.

5.6 Future work

In the future, the GPS anomaly detection and risk classification software framework could be developed by incorporating reinforcement learning methodology for the use case of real-time GPS anomaly detection in UAS navigation.

FUNDING ACKNOWLEDGEMENT

I acknowledge the support received from the Department of Defense (DoD) for Grand Forks County's Resilience Study under Grant Award number UND0026784 for Chapter 2. GPS dropout research was supported by the Federal Aviation Administration (FAA) for the ASSURE 44 project to mitigate and detect the GPS and ADS-B dropout on Unmanned Aerial Systems (UAS) under a grant award 15-C-UAS-UND-030. The dataset was sourced by Ryan Wallace from the ASSURE 56 project about electromagnetic interference on aircraft under the grant award A56_A11L.UAS.96.

REFERENCES

[1] P. M. Hurvitz, "GPS and accelerometer time stamps: Proper data handling and avoiding pitfalls," in *Proceedings of the 1st International ACM SIGSPATIAL Workshop on Smart Cities and Urban Analytics, UrbanGIS 2015*, Association for Computing Machinery, Inc, Nov. 2015, pp. 92–97. doi: 10.1145/2835022.2835038.

[2] H. J. LeBlanc, E. Gomez, F. Hassan, and N. Alsbou, "Poster: Inter-vehicle communication assisted localization with resilience to false data injection attacks," in *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, Association for Computing Machinery, Oct. 2016, pp. 64–65. doi: 10.1145/2980100.2980111.

[3] X. Wei and B. Sikdar, "Impact of GPS time spoofing attacks on cyber physical systems," in *Proceedings of the IEEE International Conference on Industrial Technology*, Institute of Electrical and Electronics Engineers Inc., Feb. 2019, pp. 1155–1160. doi: 10.1109/ICIT.2019.8755016.

[4] Federal Aviation Administration, "FAA Statements on 5G," 2022. [Online]. Available: https://www.faa.gov/newsroom/faa-statements-5g

[5] P. Phister, S. Jackson, R. Turner, J. Snoderly, and A. Squires, "System Resistance to Electromagnetic Interference." [Online]. Available: http://www.fcc.gov

[6] A. Afaq, N. Haider, M. Z. Baig, K. S. Khan, M. Imran, and I. Razzak, "Machine learning for 5G security: Architecture, recent advances, and challenges," *Ad Hoc Networks*, vol. 123, Dec. 2021, doi: 10.1016/j.adhoc.2021.102667.

[7] G. Aissou, H. O. Slimane, S. Benouadah, and N. Kaabouch, "Tree-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS," in *2021 IEEE*

12th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 649–653. doi: 10.1109/UEMCON53757.2021.9666744.

[8] J. Whelan, A. Almehmadi, and K. El-Khatib, "Artificial intelligence for intrusion detection systems in Unmanned Aerial Vehicles," *Computers and Electrical Engineering*, vol. 99, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107784.

[9] M. Leccadito, T. Bakker, R. Klenke, and C. Elks, "A survey on securing UAS cyber physical systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 10, pp. 22–32, Oct. 2018, doi: 10.1109/MAES.2018.160145.

[10] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter," *The Journal of Global Positioning Systems*, vol. 16, no. 1, Dec. 2018, doi: 10.1186/s41445-018-0018-3.

[11] South Dakota State University, IEEE Region 4, and Institute of Electrical and Electronics Engineers, *2019 IEEE International Conference on Electro Information Technology (EIT)*.

[12] C. Pedroso and A. Santos, "Dissemination control in dynamic data clustering for dense IIoT against false data injection attack," *International Journal of Network Management*, vol. 32, no. 5, Sep. 2022, doi: 10.1002/nem.2201.

[13] S. A. Almalki and F. T. Sheldon, "Deep Learning to Improve False Data Injection Attack Detection in Cooperative Intelligent Transportation Systems," in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 1016–1021. doi: 10.1109/IEMCON53756.2021.9623153.

[14] A. Aflaki, M. Gitizadeh, R. Razavi-Far, V. Palade, and A. A. Ghasemi, “A hybrid framework for detecting and eliminating cyber-attacks in power grids,” *Energies (Basel)*, vol. 14, no. 18, Sep. 2021, doi: 10.3390/en14185823.

[15] V. Zeufack, D. Kim, D. Seo, and A. Lee, “An unsupervised anomaly detection framework for detecting anomalies in real time through network system’s log files analysis,” *High-Confidence Computing*, vol. 1, no. 2, Dec. 2021, doi: 10.1016/j.hcc.2021.100030.

[16] S. Hubbard, A. Pak, Y. Gu, and Y. Jin, “Uas to support airport safety and operations: Opportunities and challenges,” *J Unmanned Veh Syst*, vol. 6, no. 1, pp. 1–17, 2018, doi: 10.1139/juvs-2016-0020.

[17] D. W. Matolak and R. Sun, “Air-ground channel measurements & modeling for UAS,” in *Integrated Communications, Navigation and Surveillance Conference, ICNS,* 2013. doi: 10.1109/ICNSurv.2013.6548539.

[18] J. Sadovskis and A. Aboltins, “Modern methods for UAV detection, classification, and tracking,” in *2022 IEEE 63rd Annual International Scientific Conference on Power and Electrical Engineering of Riga Technical University, RTUCON 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/RTUCON56726.2022.9978860.

[19] J. H. Mott, Z. A. Marshall, M. A. Vandehey, M. May, and D. M. Bullock, “Detection of Conflicts Between ADS-B-Equipped Aircraft and Unmanned Aerial Systems,” *Transp Res Rec*, vol. 2674, no. 1, pp. 197–204, Jan. 2020, doi: 10.1177/0361198119900645.

[20] R. J. Wallace, J. M. Robbins, J. M. Loffi, J. K. Holliman, D. S. Metscher, and T. R. Rogers, “Evaluating LAANC utilization & compliance for small unmanned aircraft systems in controlled airspace,” *International Journal of Aviation, Aeronautics, and Aerospace*, vol. 7, no. 2, 2020, doi: 10.15394/IJAAA.2020.1453.

[21] A. Alsoliman, G. Rigoni, D. Callegaro, M. Levorato, C. M. Pinotti, and M. Conti, "Intrusion Detection Framework for Invasive FPV Drones Using Video Streaming Characteristics," *ACM Transactions on Cyber-Physical Systems*, Jan. 2023, doi: 10.1145/3579999.

[22] E. Valovage, "Enhanced ADS-B research," in *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, 2006. doi: 10.1109/DASC.2006.313672.

[23] J. Zhang, W. Liu, and Y. Zhu, "Study of ADS-B data evaluation," *Chinese Journal of Aeronautics*, vol. 24, no. 4, pp. 461–466, Aug. 2011, doi: 10.1016/S1000-9361(11)60053-8.

[24] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models," *IEEE Access*, vol. 9, pp. 93803–93815, 2021, doi: 10.1109/ACCESS.2021.3089847.

[25] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "Softran: Software defined radio access network," *HotSDN 2013 - Proceedings of the 2013 ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, pp. 25–30, 2013, doi: 10.1145/2491185.2491207.

[26] M. Höyhtyä, O. Apilo, and M. Lasanen, "Review of latest advances in 3GPP standardization: D2D communication in 5G systems and its energy consumption models," *Future Internet*, vol. 10, no. 1, 2018, doi: 10.3390/fi10010003.

[27] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, 2014, doi: 10.1109/MCOM.2014.6736761.

[28] H. Fourati, R. Maaloul, and L. Chaari, *A survey of 5G network systems: challenges and machine learning approaches*, vol. 12, no. 2. Springer Berlin Heidelberg, 2021. doi: 10.1007/s13042-020-01178-4.

[29] E. O'Connell, D. Moore, T. N.- Telecom, and undefined 2020, "Challenges associated with implementing 5G in manufacturing," *mdpi.com*, Accessed: Feb. 27, 2022. [Online]. Available: https://www.mdpi.com/2673-4001/1/1/5

[30] J. A. Khan and M. M. Chowdhury, "Security Analysis of 5G Network," *IEEE International Conference on Electro Information Technology*, vol. 2021-May, pp. 1–6, 2021, doi: 10.1109/EIT51626.2021.9491923.

[31] A. Osseiran, J. F. Monserrat, and P. Marsch, *5G mobile and wireless communications technology*. 2016. doi: 10.1017/CBO9781316417744.

[32] V. G. Nguyen, K. J. Grinnemo, J. Taheri, and A. Brunstrom, "A Deployable Containerized 5G Core Solution for Time Critical Communication in Smart Grid," *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops, ICIN 2020*, no. Icin, pp. 153–155, 2020, doi: 10.1109/ICIN48450.2020.9059397.

[33] J. Li, K. Nagalapur, E. Stare, … S. D. preprint arXiv, and undefined 2021, "5G New Radio for Public Safety Mission Critical Communications," *arxiv.org*, 2021, Accessed: Feb. 27, 2022. [Online]. Available: https://arxiv.org/abs/2103.02434

[34] M. Patzold, "The Benefits of Smart Wireless Technologies [Mobile Radio]," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 5–12, 2017, doi: 10.1109/MVT.2017.2753080.

[35] N. Goud, "https://www.cybersecurity-insiders.com/cyber-attack-disrupts-vodafone-portugal-entire-4g-and-5g-network/," *Cybersecurity Insiders*, 2022. [Online]. Available: https://www.cybersecurity-insiders.com/cyber-attack-disrupts-vodafone-portugal-entire-4g-and-5g-network/

[36] J. Greig, “Vodafone Portugal hit with cyberattack affecting 4G/5G network, TV, SMS services,” *ZDNet*, 2022. [Online]. Available: https://www.zdnet.com/article/vodafone-portugal-hit-with-cyberattack-affecting-4g5g-network-tv-sms-services-and-more/

[37] D. Palmer, “Hackers are targeting telecom companies to steal 5G secrets,” *ZDNet*, 2021. [Online]. Available: https://www.zdnet.com/article/hackers-are-targeting-telecoms-companies-to-steal-5g-secrets/

[38] H. Kim, “5G core network security issues and attack classification from network protocol perspective,” *Journal of Internet Services and Information Security*, vol. 10, no. 2, pp. 1–15, 2020, doi: 10.22667/JISIS.2020.05.31.001.

[39] D. Goodin, “Microsoft catches Russian state hackers using IoT devices to breach networks,” ArsTechnica. [Online]. Available: https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

[40] A. Jain and T. Singh, “Implementing Security in I O T Ecosystem Using 5G Network Slicing and Pattern Matched Intrusion Detection System : A Simulation Study,” vol. 16, pp. 1–38, 2021.

[41] K. Zerrusen, G. Sachs, and C. Council, “The National Security Challenges of Fifth Generation (5G) Wireless Communcations. Winning the Race to 5G, Securely,” no. June, 2019, [Online]. Available: https://www.insaonline.org/wp-content/uploads/2019/06/INSA_WP_5G_v5_Pgs.pdf

[42] A. Kostopoulos *et al.*, “Use cases and standardisation activities for eMBB and V2X scenarios,” *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings*, 2020, doi: 10.1109/ICCWorkshops49005.2020.9145377.

[43] A. A. Ateya, A. Muthanna, M. Makolkina, and A. Koucheryavy, “Study of 5G Services Standardization: Specifications and Requirements,” *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, vol. 2018-Novem, pp. 2–7, 2019, doi: 10.1109/ICUMT.2018.8631201.

[44] J. Blackman, “What is mMTC in 5G NR, and how does it impact NB-IoT and LTE-M,” Fundamentals. [Online]. Available: https://enterpriseiotinsights.com/20191016/channels/fundamentals/what-is-mmtc-in-5g-nr-and-how-does-it-impact-nb-iot-and-lte-m

[45] Z. Li, H. Shariatmadari, B. Singh, and M. A. Uusitalo, “5G URLLC: Design challenges and system concepts,” *Proceedings of the International Symposium on Wireless Communication Systems*, vol. 2018-Augus, 2018, doi: 10.1109/ISWCS.2018.8491078.

[46] C. Bockelmann, N. Pratas, G. Wunder, … S. S.-I., and undefined 2018, “Towards massive connectivity support for scalable mMTC communications in 5G networks,” *ieeexplore.ieee.org*, Accessed: Feb. 27, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8360103/

[47] Cybersecurity and Infrastructure Security Agency, “Overview of Risks Introduced By 5G Adoption in the United States,” pp. 1–16, 2019.

[48] S. V Swamy and P. R. R, “Study of Security for 5G Wireless Communication Network,” no. July, pp. 3800–3802, 2020.

[49] National Institute of Standards and Technology (NIST), “Computer Security Resource Centre,” Glossary. [Online]. Available: https://csrc.nist.gov/glossary/term/passive_attack

[50] Positive Technologies, “Cybersecurity 2020 - 2021,” 2021. [Online]. Available: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity_20-21.pdf

[51] AdaptiveMobile, “A Slice in Time,” 2021. [Online]. Available: https://blog.adaptivemobile.com/5g-network-slicing-vulnerability-denial-of-service-attacks

[52] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, “Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities,” *IEEE Internet Things J*, vol. 6, no. 5, pp. 8169–8181, 2019, doi: 10.1109/JIOT.2019.2927379.

[53] Y. Arjoune and S. Faruque, “Smart Jamming Attacks in 5G New Radio: A Review,” *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, pp. 1010–1015, 2020, doi: 10.1109/CCWC47524.2020.9031175.

[54] JEM Engineering, “An Introduction to Jammers,” 2019. [Online]. Available: https://jemengineering.com/blog-an-introduction-to-jammers/

[55] M. A. Hasnat, S. T. A. Rurnee, M. A. Razzaque, and M. Mamun-Or-Rashid, “Security Study of 5G Heterogeneous Network: Current Solutions, Limitations Future Direction,” *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, pp. 7–9, 2019, doi: 10.1109/ECACE.2019.8679326.

[56] Q. Qiu, S. Liu, S. Xu, S. Y.-W. C. and Mobile, and undefined 2020, “Study on security and privacy in 5G-enabled applications,” *hindawi.com*, Accessed: Feb. 27, 2022. [Online]. Available: https://www.hindawi.com/journals/wcmc/2020/8856683/

[57] A. Shaik, R. Borgaonkar, S. Park, and J. P. Seifert, “New vulnerabilities in 4G and 5G cellular access network protocols : Exposing device capabilities,” in *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 221–232. doi: 10.1145/3317549.3319728.

[58] G. Sahu and S. S. Pawar, “Security Challenges in 5G Network,” in *EAI/Springer Innovations in Communication and Computing*, 2022, pp. 75–94. doi: 10.1007/978-3-030-91149-2_4.

[59] J. Hamamreh, “Physical Layer Security Against Eavesdropping in The Internet of Drones (IoD) Based Communication Systems,” pp. 1–7, 2019.

[60] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, “On the security of the 5G-IoT architecture,” *ACM International Conference Proceeding Series*, 2018, doi: 10.1145/3269961.3269968.

[61] G. Holtrup, W. Lacube, D. P. David, A. Mermoud, G. Bovet, and V. Lenders, “5G System Security Analysis,” no. August 2021, pp. 1–47, 2021, [Online]. Available: http://arxiv.org/abs/2108.08700

[62] I. ul haq, J. Wang, and Y. Zhu, “Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks,” *Journal of Network and Computer Applications*, vol. 161, no. February, pp. 1–11, 2020, doi: 10.1016/j.jnca.2020.102660.

[63] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues, “Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3047895.

[64] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, “Secure D2D communication for 5G IoT network based on lightweight cryptography,” *Applied Sciences (Switzerland)*, vol. 10, no. 1, Jan. 2020, doi: 10.3390/app10010217.

[65] B. Yang, T. Taleb, Z. Wu, and L. Ma, “Spectrum Sharing for Secrecy Performance Enhancement in D2D-Enabled UAV Networks,” *IEEE Netw*, vol. 34, no. 6, pp. 156–163, Nov. 2020, doi: 10.1109/MNET.011.2000093.

[66] H. Huang, J. Chu, and X. Cheng, “Trend Analysis and Countermeasure Research of DDoS Attack under 5G Network,” in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 153–160. doi: 10.1109/CSP51677.2021.9357499.

[67] H. A. Alamri, V. Thayananthan, and J. Yazdani, “Machine Learning for Securing SDN based 5G Network,” 2021.

[68] B. Ying, A. N.-J. of N. and C. Applications, and undefined 2019, “Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography,” *Elsevier*, Accessed: Feb. 27, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519300256?casa_token=Xy3pPlLZA9EAAAAA:NDImzMQqNHE7MDXqBU7Y-ADV1rJ84b1pWEQNouIZ3avmHg-dwQloAfcW8lzKdewEdAkGCQ

[69] M. Patzold, “The Benefits of Smart Wireless Technologies [Mobile Radio],” *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 5–12, Dec. 2017, doi: 10.1109/MVT.2017.2753080.

[70] 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*, vol. 67, no. 1, pp. 618–632, Jan. 2018, doi: 10.1109/TVT.2017.2745110.

[71] M. Awais Javed and S. khan Niazi, “5G Security Artifacts (DoS / DDoS and Authentication); 5G Security Artifacts (DoS / DDoS and Authentication),” 2019.

[72] P. Varga *et al.*, “5g support for industrial iot applications – challenges, solutions, and research gaps,” *Sensors (Switzerland)*, vol. 20, no. 3, Feb. 2020, doi: 10.3390/s20030828.

[73] A. Gupta, R. Kumar Jha, S. Jain, and A. Professor in, “Attack modeling and intrusion detection system for 5G wireless communication network,” *Wiley Online Library*, vol. 30, no. 10, Jul. 2016, doi: 10.1002/dac.3237.

[74] IEEE Communications Society and Institute of Electrical and Electronics Engineers, *2017 IEEE Conference on Standards for Communications and Networking (CSCN) : 18-20 Sept. 2017.*

[75] M. Geller and P. Nair, “Whitepaper Cisco Public 5G Security Innovation with Cisco,” 2018.

[76] J. Kamasa, “Securing Future 5G-Networks,” *Research Collection*, vol. 21, no. 6, pp. 12–19, 2020, [Online]. Available: https://doi.org/10.3929/ethz-a-010025751

[77] Institute of Electrical and Electronics Engineers, *2018 IEEE Global Communications Conference (GLOBECOM) : proceedings : Abu Dhabi, UAE, 9-13 December 2018.*

[78] A. S. Khan, Y. Javed, J. Abdullah, J. M. Nazim, and N. Khan, “Security issues in 5G device to device communication,” 2017.

[79] J. Hasneen and K. M. Sadique, “A Survey on 5G Architecture and Security Scopes in SDN and NFV,” pp. 447–460, 2022, doi: 10.1007/978-981-16-2008-9_43.

[80] IEEE Communications Society and Institute of Electrical and Electronics Engineers, *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).*

[81] S. Kwon, S. Park, H. J. Cho, Y. Park, D. Kim, and K. Yim, “Towards 5G-based IoT security analysis against Vo5G eavesdropping,” *Computing*, vol. 103, no. 3, pp. 425–447, Mar. 2021, doi: 10.1007/s00607-020-00855-0.

[82] E. T. Saglam and S. Bahtiyar, “A Survey: Security and Privacy in 5G Vehicular Networks,” in *UBMK 2019 - Proceedings, 4th International Conference on Computer*

Science and Engineering, Institute of Electrical and Electronics Engineers Inc., Sep. 2019, pp. 108–112. doi: 10.1109/UBMK.2019.8907026.

[83] M. Baza *et al.*, "Detecting Sybil Attacks Using Proofs of Work and Location in VANETs," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 1, pp. 39–53, 2022, doi: 10.1109/TDSC.2020.2993769.

[84] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," 2006.

[85] J. M. Batalla *et al.*, "Security Risk Assessment for 5G Networks: National Perspective," *IEEE Wirel Commun*, vol. 27, no. 4, pp. 16–22, Aug. 2020, doi: 10.1109/MWC.001.1900524.

[86] Q. Wu, G. Y. Li, W. Chen, D. Wing, K. Ng, and R. Schober, "An overview of sustainable green 5G networks," *ieeexplore.ieee.org*, 2016, Accessed: Feb. 27, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8014295/

[87] Huawei Technologies, "5G power whitebook," 2019, [Online]. Available: https://www.huawei.com/minisite/5g-ultra-lean-site-2019/pdf_v1.0/5G-power-cn.pdf

[88] N. Prates, A. Vergutz, R. T. MacEdo, A. Santos, and M. Nogueira, "A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic," *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, 2020, doi: 10.1109/GLOBECOM42002.2020.9322070.

[89] S. Bhasin, A. Chattopadhyay, A. Heuser, D. Jap, S. Picek, and R. R. Shrivastwa, "Mind the Portability: A Warriors Guide through Realistic Profiled Side-channel Analysis," 2020, doi: 10.14722/ndss.2020.24390.

[90] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “CISA 5G strategy: Ensuring the security and resilience of 5G infrastructure in our nation 2020,” pp. 1–24, 2020.

[91] J. Kamasa, “Securing Future 5G-Networks,” *Research Collection*, vol. 21, no. 6, pp. 12–19, 2020.

[92] National Institute of Standards and Technology (NIST), “Computer Security Resource Centre,” Glossary. [Online]. Available: https://csrc.nist.gov/glossary/term/passive_attack

[93] Federal Aviation Administration, “5G and Aviation Safety,” 5G. [Online]. Available: https://www.faa.gov/5g

[94] K. Mok, “In Defense of 5G: National Security and Patent Rights Under the Public Interest Factors,” *The University of Chicago Law Review*, vol. 86, no. 1, pp. 77–142, 2019.

[95] Department of Homeland Security, “5G Introduces New Benefits, Cybersecurity Risks,” *Science and Technology Directorate*, 2020.

[96] D. Soldani, “5G and the Future of Security in ICT,” *2019 29th International Telecommunication Networks and Applications Conference, ITNAC 2019*, 2019, doi: 10.1109/ITNAC46935.2019.9078011.

[97] National Security Agency, “Potential threat vectors to 5G infrastructure,” pp. 1–16, 2021.

[98] Positive Technologies, “Threat vector: GTP. Vulnerabilities in LTE and 5G Networks,” 2020.

[99] G. Horn and P. Schneider, “Towards 5G security,” *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, vol. 1, pp. 1165–1170, 2015, doi: 10.1109/Trustcom.2015.499.

[100] E. Rosenblatt, “Cybersecurity in 5G,” *Yale Cyber Leadership Forum*, pp. 1–6, 2021. [Online]. Available: https://cyber.forum.yale.edu/blog/2021/7/20/cybersecurity-risk-in-5g

[101] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, “5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation,” *2018 IEEE International Conference on Communications Workshops, ICC Workshops 2018 - Proceedings*, pp. 1–6, 2018, doi: 10.1109/ICCW.2018.8403769.

[102] F. Liu, J. Peng, and M. Zuo, “Toward a Secure Access to 5G Network,” *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 1121–1128, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00156.

[103] GSM Association (GSMA), “Embedded SIM Remote Provisioning Architecture,” pp. 1–113, 2020, [Online]. Available: https://www.gsma.com/esim/wp-content/uploads/2020/07/SGP.01-v4.2.pdf

[104] GSMA, “IoT Security Guidelines Overview,” *IoT Security Guidelines*, vol. 2.2, 2020.

[105] B. Garner, “What’s a Sybil Attack & How Do Blockchains Mitigate Them?,” Coin Central. [Online]. Available: https://coincentral.com/sybil-attack-blockchain/

[106] J. R. Douceur, “The Sybil Attack,” *Microsoft Research*, p. 259, 2002, doi: 10.1145/984622.984660.

[107] L. Li, S. Das, R. J. Hansman, R. Palacios, and A. N. Srivastava, “Analysis of flight data using clustering techniques for detecting abnormal operations,” in *Journal of Aerospace Information Systems*, American Institute of Aeronautics and Astronautics Inc., 2015, pp. 587–598. doi: 10.2514/1.I010329.

[108] K. Sheridan, T. G. Puranik, E. Mangortey, O. J. Pinon, M. Kirby, and D. N. Mavris, “An application of dbscan clustering for flight anomaly detection during the approach phase,” in *AIAA Scitech 2020 Forum*, American Institute of Aeronautics and Astronautics Inc, AIAA, 2020. doi: 10.2514/6.2020-1851.

[109] M. Y. Chesnokov, “Time Series Anomaly Searching Based on DBSCAN Ensembles,” *Scientific and Technical Information Processing*, vol. 46, no. 5, pp. 299–305, Dec. 2019, doi: 10.3103/S0147688219050010.

[110] M. Ankerst, M. M. Breunig, H.-P. Kriegel, and J. Sander, “OPTICS: Ordering Points To Identify the Clustering Structure,” 1999.

[111] Z. Deng, Y. Hu, M. Zhu, X. Huang, and B. Du, “A scalable and fast OPTICS for clustering trajectory big data,” *Cluster Comput*, vol. 18, no. 2, pp. 549–562, Jun. 2015, doi: 10.1007/s10586-014-0413-9.

[112] X. Zhu *et al.*, “A Noise Removal Algorithm Based on OPTICS for Photon-Counting LiDAR Data,” *IEEE Geoscience and Remote Sensing Letters*, vol. 18, no. 8, pp. 1471–1475, Aug. 2021, doi: 10.1109/LGRS.2020.3003191.

[113] D. Reynolds, “Gaussian Mixture Models *.”

[114] B. Chettri and B. L. Sturm, “A Deeper Look at Gaussian Mixture Model Based Anti-Spoofing Systems,” in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Sep. 2018, pp. 5159–5163. doi: 10.1109/ICASSP.2018.8461467.

[115] M. Łuczak, “Hierarchical clustering of time series data with parametric derivative dynamic time warping,” *Expert Syst Appl*, vol. 62, pp. 116–130, Nov. 2016, doi: 10.1016/j.eswa.2016.06.012.

[116] A. M. Bagirov, R. M. Aliguliyev, and N. Sultanova, “Finding compact and well-separated clusters: Clustering using silhouette coefficients,” *Pattern Recognit*, vol. 135, Mar. 2023, doi: 10.1016/j.patcog.2022.109144.

[117] P. J. Rousseeuw, “Silhouettes: a graphical aid to the interpretation and validation of cluster analysis,” 1987.

[118] S. P. Petrovi´c, “A Comparison Between the Silhouette Index and the Davies-Bouldin Index in Labelling IDS Clusters.”

[119] R. J. Wallace, K. M. Kiernan, T. Haritos, J. Robbins, and J. M. Loffi, “Evaluating Small UAS Operations and National Airspace System Interference Using AeroScope,” *Journal of Aviation Technology and Engineering*, vol. 8, no. 2, p. 24, May 2019, doi: 10.7771/2159-6670.1189.

[120] J. A. Besada, I. Campaña, D. Carramiñana, L. Bergesio, and G. de Miguel, “Review and simulation of counter-uas sensors for unmanned traffic management,” *Sensors*, vol. 22, no. 1, Jan. 2022, doi: 10.3390/s22010189.

[121] B. Choi and D. Oh, “Classification of Drone Type Using Deep Convolutional Neural Networks Based on Micro- Doppler Simulation; Classification of Drone Type Using Deep Convolutional Neural Networks Based on Micro- Doppler Simulation,” 2018.

[122] B. Taha and A. Shoufan, “Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research,” *IEEE Access*, vol. 7, pp. 138669–138682, 2019, doi: 10.1109/ACCESS.2019.2942944.

[123] S. Poikonen and J. F. Campbell, “Future directions in drone routing research,” *Networks*, vol. 77, no. 1, pp. 116–126, Jan. 2021, doi: 10.1002/net.21982.

[124] M. Grandini, E. Bagli, and G. Visani, “Metrics for Multi-Class Classification: an Overview,” Aug. 2020, [Online]. Available: http://arxiv.org/abs/2008.05756

[125] C. Yang, Y. Wang, Y. Zhou, J. Ruan, and W. Liu, “False Data Injection Attacks Detection in Power System Using Machine Learning Method,” *Journal of Computer and Communications*, vol. 06, no. 11, pp. 276–286, 2018, doi: 10.4236/jcc.2018.611025.