Radio Cyber Intrusion Detection in CBTC Train Network

SUPERIOR UNIVERSITY

MS ELECTRICAL ENGINEERING

BY

MUHAMMAD ASIM

Roll No: MSEE-F21-007

SEASON 2021-2023

DEPARTMENT OF ELECTRICAL ENGINEERING

SUPERIOR UNIVERSITY

Lahore, Pakistan

Radio Cyber Intrusion Detection in CBTC Train Network

SUPERIOR UNIVERSITY

MS ELECTRICAL ENGINEERING

BY

MUHAMMAD ASIM

Roll No: MSEE-F21-007

SEASON 2021-2023

SUPERVISOR **Dr. Saif Ur Rehman**

DEPARTMENT OF ELECTRICAL ENGINEERING
SUPERIOR UNIVERSITY

Lahore, Pakistan

Abstract

In day by day increasing the population needs more and more safe, reliable, green energy transportation, time-saving, and the cheapest transport system for making a better lifestyle that's why introducing a Communication Based Train Control (CBTC) system, therefor an upgradation method of Traction Based Train control (TBTC) (because some time term is using a CBTC improving technology of TBTC). The CBTC network uses many components for making the whole system, likely first one is the train onboard network which further consists of a Vehicle On-Board Controller/Computer (VOBC), Onboard Automatic Train protection (ATP), and Automatic Train operation (ATO) Automatic Train supervision (ATS) zone controller (ZC) and Radio Communication System (RCS) second is Train-to-trackside radio network and the third one is Trackside backbone network for minimum headway for safe traveling network. Currently the CBTC system working on the train to trackside network. The primary functions are carried by wireless communication, which is implementing the communication between Ground and Train. However, this system is involving too large infrastructure interface and subsystems which is making the complex equipment system and having a higher rate of maintenance. In this work discuss about train-to-train communication (T2T) which is a better improvement in the CBTC network. Also, work on the radio intrusion detection method IDE (Intrusion detection systems to protect the vital role of the system against cyber-attacks). And improving results in CBTC trainto-train communication. Currently work is done on IEEE 802.11 protocol on the train to trackside equipment RID. In this work, we will make an algorithm for train-to-train communication RID on the base of protocol IEEE 802.11 work on its typical, behavior, critical, and respective class issues. In the end, this work prove how we will distinguish the effect attack types in train-to-train communication systems and make more reliable systems in the transport networks.

Copyright © 2023 by Author

All rights are reserved to the author. No part of this dissertation may be copied, recorded, reproduced, distributed, or transmitted in any form or by any means, including electronic or other means. Any information should not be stored or retrieved without the prior written permission of the author.

Muhammad Asim

Dated:

DEDICATION

To ALLAH the Almighty

&

To My Parents Teachers & Family

RESEARCH COMPLETION CERTIFICATE

It is certified that the research work contained in this dissertation titled "**Radio Cyber Intrusion Detection in CBTC Train Network**" has been investigated and carried out by **Mr. Muhammad Asim** Roll No. **MSEE-F21-007** under my supervision. Therefore, the undersigned hereby certify that they have read and recommended the dissertation entitled for the degree of Master of Science in Electrical Engineering.

EXAMINATION JURY/BOARD APPROVAL

Sr No	Name	Role	Signature
1	Dr. Mustafa Shakir	Chairman	
2	Dr. Saif Ur Rehman	Thesis Supervisor	
3	Dr. Mustafa Shakir	Internal Examinar-1	
5	Dr. Manzoor Elahi	Internal Examinar-3	

AUTHOR’S DECLARATION

I, **Muhammad Asim** Roll No. **MSEE-F21-007** student of Department of **Electrical Engineering**, Superior University, Lahore in the subject of MS Electrical Engineering Session 2021-2023, hereby declare that the matter printed in the dissertation as “**Radio Cyber Intrusion Detection in CBTC Train Network**” is my research work. The text and results mentioned in this dissertation have not been printed, published, or submitted in any form at any national or international organization. I hereby certify that this research does not involve any plagiarized material or results that another person has published. My colleagues and friends assisted me while carrying out this research. I identified their contribution as well. If it contains any plagiarized information, I bear full responsibility.

Signature:

Date:

PLAGIARISM UNDERTAKING

I solemnly state that the research work illustrated in this dissertation titled "**Radio Cyber Intrusion Detection in CBTC Train Network**" is my work without any remarkable contribution of any other person. Small contribution taken from any colleague has been duly acknowledged and stated clearly.

I also recognize the zero-tolerance policy of the HEC and Superior University, Lahore, towards plagiarism. Therefore, as an author of the above-titled dissertation, I declare that this research does not involve any plagiarized material or results that another person has published, and any material used as a reference is correctly cited in the bibliography section.

I bear complete responsibility that if I am found guilty of any formal plagiarism in the above-titled dissertation even after the award of my degree, the University reserves the right to revoke my degree at any stage. Furthermore, HEC and the University have the right to declare blacklisted at any forum.

Name: Muhammad Asim

Dated

CERTIFICATE

I certify that I have ensured that ____________ has complied with the regulations for higher degrees. I also certify that the research work embodied in this dissertation entitled "**Radio Cyber Intrusion Detection in CBTC Train Network**" has been carried out by ___________ under my supervision and is worth presenting to Superior University Lahore, Pakistan.

Dr. Saif Ur Rehman ______________________________

Assistant Professor **(Supervisor)**

Department of Electrical Engineering

Superior University, Lahore

ACKNOWLEDGEMENTS

I would like to express my gratefulness to Almighty **ALLAH** and the Holy Prophet **MUHAMMAD P.B.U.H.** for giving me strength and helping me achieve my goal of life about which I just imagined.

I would like to express my deep and sincere gratitude to my supervisor **Dr. Saif Ur Rehman**,

MUHAMMAD ASIM

Table of Content

Contents

Keywords

CBTC	Communication Base Train Control
TBTC	Track Base Train Control
AC	Alternating Current
AF	Audio Frequency
ATS	Automatic Train Supervision
ATP	Automatic Train Protection
ATC	Automatic Train Control
ZC	Zone Controller
SA	Station Adopter
OCC	Operation Control Center
MA	Movement Authority
T2W	Train to Way Side
T2T	Train to Train

CHAPTER 1

INTRODUCTION

1.1 Introduction:

In the modern era, time and money are the major concerns of a human being for a safer and least expensive transport system. Communication-based train control (CBTC) addresses these factors comfortably and is receiving increasing amounts of attention daily also in day by day increasing the population and rises fuel prices needs more and more safe, reliable, green energy transportation, time-saving, and the cheapest, economical transport system for making a better modern world and lifestyle. Traditional rail system is working on fixed path that's way it has been characterized with less friction on rail with poor brake system capacities and remove obstacles. On these reason this system of train control is cause to derailing and colliding. The world is move to traditional rail system to CBTC system is subway intracity or intercity transport also. Chapter 1 is describes the introduction of Communication Base Train Control CBTC its all function and parameters in this thesis work. It is started with the basic of CBTC In the next section the work describes the background of the research work.

This study aims to introduce the radio intrusion detection method IDE Train-to-train communication (T2T), which is a better improvement in the CBTC network to protect the vital role of the system against cyberattacks. Currently, work is being done on the IEEE 802.11 protocol on trains to trackside equipment RID. This work proved the radio intrusion detection method which is based on M-gram Modal by using the machine learning technique on data set of CIC-IDS2017 which gives the better improvement in communication systems and made more reliable systems in transport networks.

1.2 Background:

In the modern era, the rapid advancement of wireless communication and Internet of Things (IoT) technologies has transformed various sectors, including transportation, healthcare, and industrial systems. Technologies that underlie CBTC are as follows CBTC systems, which employ these technologies, are observed to provide invaluable enhancements in the operation of trains. But, with these improvements come increased vulnerability to cyber attacks and this, requires adequate measures to enhance the security of infrastructure.

As mentioned earlier, with the merging of wireless communication and IoT in the operation of CBTC systems, new threats appear to be more attractive for cyber-attacks. Wireless communication and IoT security have been an issue of concern in many research works due to the increased cases of cybercrimes that require better and improved security measures and better intrusion detection mechanisms. For example, Ghadi et al (2024) discuss the issues and recommendations about safe Health 4. 0 instruments based on 5G and MEC structures and the significance of safe data transfer in the IoT [1]. Likewise, different techniques of the machine learning approach have been proposed for dealing with security problems in wireless sensor networks as observed in [2] proving a worth of the artificial intelligence in the improvement of the network security.

Growing usage of IoT and wireless communication in SCADA systems such as smart grid and industrial control systems (ICS) are also main drivers for proper IT security systems to be implemented. Ali et al. (2023) have developed an ICS-IDS for detecting cyber attacks in ICS networks to prove big data analysis and machine learning's capability in detecting various complex threats [3]. In addition, the authors of [4] discuss IoT security threats and present AI approaches to mitigate them; special attention is given to the use of deep learning for protecting IoT devices. With regards to countering cyber threats in modern networks, the approach presented in [5] on the application of both the machine learning and the blockchain methods on smart grid security can also be regarded as innovative.

The objective of this research is to propose a new radio intrusion detection method, IDE T2T, to improve the security of CBTC networks from cyber threats. Using complex techniques in ML and big data analysis, this paper aims at establishing a more dependable and less vulnerable CBTC system that will enhance the efficiency of trains leading to safer means of transport.

1.3 Scientific Contribution

The main contributions may be summarized as follows:

Introduction of a Novel Intrusion Detection Method: This work proposes a novel approach to RIDD for the T2T communication in CBTC systems. This method improves the viability of CBTC systems against cyber threats and attacks in the following ways.

Application of Machine Learning Techniques: Applying machine learning to the identification and classification of cyber intrusions, the research uses the Gradient Boosting Classifier method.

It can be clearly seen that the above-mentioned approach outperforms other previously used methodologies with a higher rate of correct identification and lower false positive rates.

Comprehensive Evaluation and Simulation: The evaluation of the proposed intrusion detection method is carried out through simulations on the CIC-IDS2017 and AWID datasets. The findings demonstrate the way by which the method enables the detection of multiple forms of attacks such as the DoS attack, injecting attacks and impersonation attacks.

Analysis of CBTC Network Vulnerabilities: Consequently, the study gives a detailed description of weaknesses in the CBTC networks and stresses the importance of adequate security measures. It states major risks, namely, the low level of encryption and a lack of necessary authentication and answers to these problems.

Development of a Cyber Detection System: An ADS for purely computerized systems using the modal M-gram is constructed and its capacity to detecting abnormities in train communication systems is demonstrated. This system improves the protection of CBTC networks by offering near real-time identification of invasion.

Proposed Solutions for Technical Challenges: Several technical issues are discussed in the research concerning CBTC networks, while the proposed solutions include the incorporation of detection models associated with the devices' states and the development of an HMM classifier to separate faults from attacks.

Altogether, these contributions contribute to enhance the existing literature and increase the awareness of the threats in railway communication system, establish a base for the future studies and practical applications to protect critical area.

1.4 Composition of the Article

This paper is divided into seven sections each of which deals with some crucial issues concerning the comparative study of cyber intrusion in radio CBTC train networks. Section one gives the background to the research topic and discusses the importance of increasing the levels of security in the contemporary train control systems. Chapter 2 provides an overview of the related work, which presents a literature survey on the security of CBTC and the approaches to intrusion detection. And the problem of the current CBTC systems and reveals the presented deficiencies that require the proposed enhancements. Chapter 3 presents the methodology, detailing the novel intrusion detection approach and the machine learning techniques employed in this study. Chapter 4 discusses the experimental setup and the datasets used for evaluation, providing insights into the data collection and preprocessing steps into radio intrusion detection, explaining the mechanisms and strategies implemented to detect and mitigate intrusions. also presents the results and analysis, showcasing the effectiveness of the proposed method through comprehensive simulations and comparisons with traditional techniques. Finally, Chapter 5 concludes the article by summarizing the key findings, discussing the implications for future research, and proposing potential enhancements to further secure CBTC systems.

1.5 Current Research

With increasing population and increasing fuel prices, increasingly safe, reliable, green energy transportation, time-saving, and inexpensive, economical transport systems are needed to improve the modern world and lifestyle. A traditional rail system operates on a fixed path characterized by less friction on the rail with poor brake system capacities and obstacle removal. For this reason, this system of train control causes derailing and colliding. The world is moving from traditional rail systems to CBTC systems through subway intracity or intercity transport. CBTC functions and parameters are introduced in this study. This section starts with the basic CBTC. In the next section, the work describes the background of the research. Traditional railway technology is nearly expired and only half a century old; it works on signal systems and detects train locations with axle counters and track circuits. Currently, the number of unexpected delays and accidents in train transportation systems are increasing daily. This is the major reason the world is required to move traditional railway systems to modern railway systems [6]. The traditional rail system is based on a fixed block system, and the modern rail system is based on a moving block system. The modern era of railway systems using communication for transferring and controlling real-time information from trains to track this term is called a radio communication-based signal system. Using real-time information, we were able to safely reduce the line capacity of two trains (headways). The headway is the time span and distance between two trains on the same line in the same time period. Today, in mass transit system communication-based train control, CBTC is the first priority of railway systems. CBTC has more than one hundred systems worldwide [7]. In Pakistan, the first CBTC transit system, called the orange line metro rail transit system, was installed under the Chinese Joint Venturi JV of Norinco International, Guangzhou Metro and Daewoo Pakistan. In a study, the European rail system increased from approximately 122 billion euros per year to approximately 150 euros between 2008 and 2013 and increased to 176 euros per billion in 2017, and on the basis of modern communication-based signal systems, CBTC trains were installed at approximately 1077.80 km on the rail track between 2011 and 2021; if we compare 2001 to 2010, only 188.9 km [8].

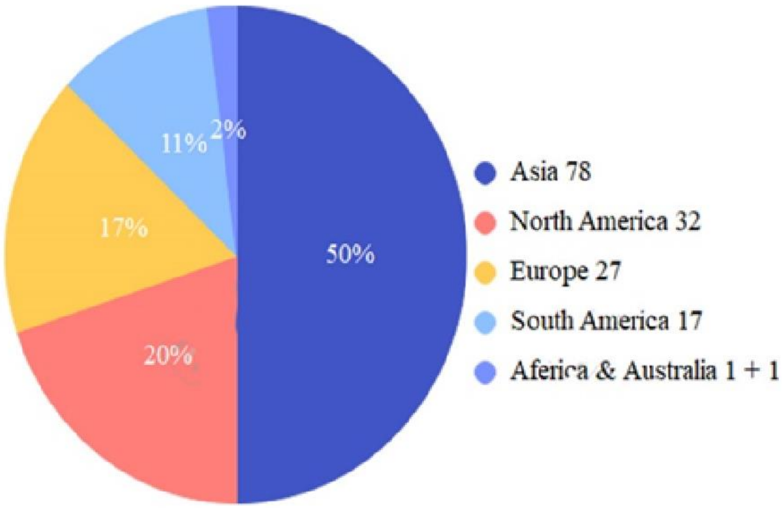

Figure 1: CBTC Project Worldwide [8]

Figure 1 shows that approximately 156 subway lines were constructed using CBTC signal systems. Almost half of the CBTC systems are installed in Asia, China, India and Japan have many subway lines, and many lines use modern CBTC technology. Pakistan has also installed its First CBTC Line in Lahore, known as the Orange Line Metro Rail Transit. The USA and European countries also used the CBTC signal system in their subway network. The most important metro lines used the CBTC: Shanghai, Guangzhou, Beijing, Singapore, Hong Kong, Tokyo, Kuala Lumpur, Delhi, etc., which also used CBTC signaling systems from Asia. Yuksel, T. and Ozturk, Z. CBTC projects worldwide. From Europe, Paris, Barcelona, Madrid, Istanbul, London (Umraniye, Kadıkoy-Kartal, Uskudar, Marmaray), Amsterdam, Munich, etc., used CBTC technology lines. In America, the CBTC lines used are the New York, Vegas, San Francisco, Buenos Aires, Las Mexico City, and Sao Paulo CBTC subway lines. In Europe, CBTC systems are used with the European Train Control System (ETCS) [7]. For example, they are used together in two technologies [9]. Some of the major cities that have implemented or are in the process of implementing CBTC systems include New York City, London, Paris, Singapore, Hong Kong, Toronto, and Beijing. In New York City alone, the Metropolitan Transportation Authority has been gradually implementing

CBTC on several of its subway lines, with plans to have the technology installed on all subway lines by 2030. CBTC systems are also being implemented in other types of transit systems, such as light rail and commuter rail. For example, the Regional Transportation District in Denver, Colorado, has installed a CBTC system on its E, F, and R light rail lines, while the San Francisco Bay Area Rapid Transit (BART) system has implemented CBTC on its A and B lines [10].

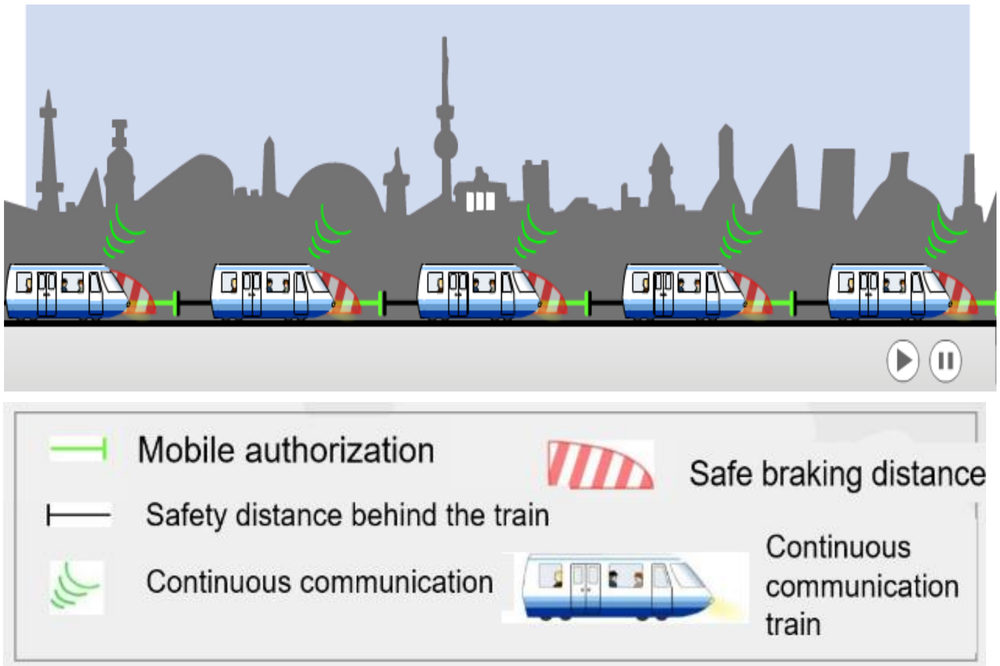

Figure 2. Overview of a CBTC System

Figure 2 shows the generic phenomena of the CBTC network. Mobile authorization in CBTC on the other hand is employed for activities such as configuration, maintenance and diagnosing of the system. It enables officially authorized individuals to be able to operate some of the equipment that is on the train from a distance without having to get into the train cab. Thus, the safety distance depends on such parameters: the maximum allowed speed of a train, train's braking characteristics, and characteristics of the signal and safety system. In the cases of CBTC systems, the distance is usually measured by the wayside signaling system and it will be in contact with the onboard equipment of each train. Especially in CBTC, there should be continuous communication between the train and the underlying architecture in order to allow the communication system to adapt real time speed and distance commands to allow train separation. It also gives real time information on the behavior of the train to the system to help in the helping in formulation of train schedules and determine early signs of danger on the train before they become a safety issue. If safe braking distance is infringed, then the onboard equipment will apply brakes to the train in a bid to stop it.

This is a very important safety consideration that guarantees that trains can run safely even in the event where the train exhibits negative responsiveness such as a halt, or in the event that the equipment that is on the train fails [11].

1.6 Research Gap

Nevertheless, there are certain research gaps that exist even to date with respect to CBTC systems and these gaps are preventing realization of all the said benefits. This especially if one considers cybersecurity. An indication that such gaps exist should serve as a justification for the efforts proposed by this work.

The major point is that the current CBTC systems are still open to cyberattacks because of lack of encryption protocols and poor authentication means. Despite the many intrusion detection techniques that have been suggested, their applicability in real time scenarios with train-to-train communication is somewhat wanting. Not having proper radio communication-based intrusion detection system for CBTC networks has indeed been a big gap in earlier works.

The area of machine learning applied for the improvement of cybersecurity in CBTC systems has not been given a 100% effort. While some research work has been done to apply artificial intelligence in intrusion detection, it is noted that the few studies available have yet to show beyond doubt the superiority of these AI methods over other classical approaches through exhaustive evaluations. This gap only underscores the need for sophisticated machine learning algorithms that can identify cyber intrusions with high precision and later classify them based on a low false positive rate.

The evaluation of intrusion detection systems in third place is not representative of the actual circumstances with which the CBTC networks are faced in the world. Most research work is based on generic datasets that do not address specific features and challenges of CBTC communication, making it difficult to come up with cybersecurity solutions that would be effective for such a specialized system like CBTC.

In addition, an essential technical problem is the differentiation between failures and cyber incidents on CBTC networks that leads to a safety and security issue. Most existing detection models lack such capability and therefore are unable to guarantee the proper functioning which results in ineffectiveness of typical detection strategies, ultimately leaving us without a comprehensive solution.

The completion of comprehensive cybersecurity in CBTC networks is the last item in their to-do list and quite neglected. Current methodologies tend to concentrate on individual components of security to be it encryption or anomaly detection alone, without even an inch for the all-encompassing connection between multiple strata at a layered level. The fragmented approach does not allow this powerful protection is which can be provided only by a unified whole system and as such, fails to safeguard the critical railway infrastructure that it ought to uphold.

The absence of these research gaps justifies the contributions that we make in this study. Our primary focus is on curbing these limitations by introducing a unique radio intrusion detection technique that seeks help from sophisticated machine learning strategies, and going through thorough evaluations with actual datasets. With the elimination of these gaps, this work paves its way to ensuring the development of highly secure and dependable CBTC system is playing a significant role in elevating the safety as well as operational standards for modern rail transport systems.

1.7 Fixed Block And Moving Block

In fixed block traditional railway system first is track divided into two parts one is track section block and other is track circuit is installed for verification the train is inside of the track of this block. When train is in the block it's not giving any method to determination of real time data like not giving exact location in the block because in occupied block considered as a full load in the line and block signal not allowed to enter any other train in this block. In this system block are fixed the entered train fixed braking capabilities and fixed speed. Signal is giving the protection of each single block. Every signal is decided the length of block, how line distance, speed limit allowed in this block line on this base of track circuit called a fixed block operation [4]. In moving block signal operation has no fixed boundaries. In implementation of CBTC giving the real time data of train through track side component. The train continuously send the real time data and location send the Operation control Center that's implementation allows the multi train on one track on shorter headway with safety. The signal system detects the position of the front and rear trains through continuous wireless communication between the trackside and the train's AP antenna, and calculates the corresponding protection distance to achieve the safety protection and automatic control of the front and rear trains. This blocking method is called mobile blocking method. In this closed system, the interval between trains is not fixed, as long as the subsequent trains have corresponding braking distances and protective distances, so that the traffic density is greatly improved. Figure 2 shows the main Difference of Fixed Block and Moving Block System.

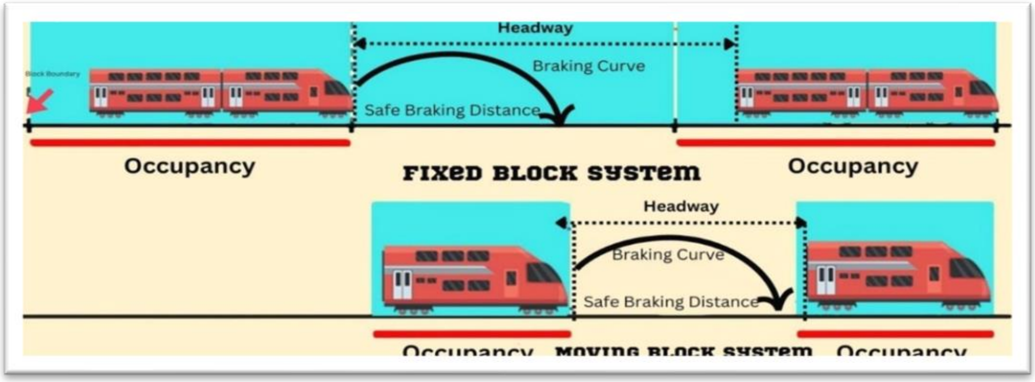

Figure 3: Fixed Block and Moving Block

In this diagram fixed block system has fixed headway and fixed breaking curve apply brake on fix safe distance but the other hand moving block not a fixed distance in this system the traction and braking capabilities depend on next upfront train. If the upfront train is coming slow or back word train is going fast the back work train speed is automatically reduce when its reach to safe distance if the train is exceed the safe distance then the train automatically system immediately apply the emergency brake.

1.8 Signaling System:

Previously, the rail system started with the traditional rail system. This method works on a fixed block system but involves the evolution of a track circuit, which is called TBTC track base train control. AC alternating current covered in the audio frequency. Cab signaling sends the control data to the driver inside the train and forces the permitted speed to control the train. Referring to the track circuit signal helps determine the train location via the signal. This technology, called track-based train control, was first used for communication between trains. In this system, the line capacity is too low because less communication of train information that sways the headway is larger and too long. For these reasons, the headway consisted of several minutes [13]. In the 1980s, the CBTC system was introduced as an inductive base loop in communication technology called signaling system transmission-based train control [12]. This system uses one advance step of the traditional rail system. In this system, inductive loop cables were mounted on regular track intervals, which were coded at a certain frequency. The detector is mounted on the base of the train. These detectors read the specific signal and verify the train location. In 1985, the first inductive CBTC technology system was installed in Toronto, Canada, at the Scarborough RT line Toronto transit commission [7]. In 1983, Lille Light Metro installed an early CBTC of inductive loop-based signals, and in 1998, the first service line was installed on Paris Line 14 [13]. Inductive loop system technology has been needed for approximately two to three decades but uses nonstandard unshielded wires and is cost-effective, easy to install and easy to repair. The initial cost is high, and the conductor is at risk. Modern CBTC systems, which operate in the GHz frequency range instead of the inductive loop system at KHz [14], have been developed. As we previously discussed, modern CBTC networks work on moving blocks. This system uses radio communication for high-capacity transmission to obtain accurate train control information between the sides and trains. Getting accurate train information provides a shorter headway and increases the line capacity. Increasing the CBTC provides a typical headway of 90 seconds or less, and in Pakistan, the current minimum headway is 5 minutes and 30 seconds [15, 16]. Moreover, in advance, the CBTC network provides operator-less and nondriver train operation [17]. In 2003, the first advanced CBTC network on a radio basis was installed at the San Francisco airport, which was provided by Bombardier [7]. In 2018, the first advanced CBTC network was installed in Lahore, Pakistan. CBTC systems have been mostly installed, particularly intracity modern subway line systems

1.9 Traditional Rail Signal System:

The pure traditional rail signal system is work on fixed block method but after evolving the track circuits it's modified to track base train control TBTC. In this evolving system using of alternating current AC which is further called Audio Frequency AF used communication between the wayside and train infrastructure. In the range of audio frequency to modulate the data of train in the range of frequency. Cab signaling send the control data to driver inside the train and forcing the permitted speed to control the train. Referring the track circuit signal helps the determination on train location via signal. This technology is earlier using for communication the train called track based train control. In this system the line capacity is too low due to less communication of train information that sway the headway is larger and too long. Due to all of these reasons the headway consisting of several minutes [3].

1.9.1 Inductive loop based CBTC:

In 1980's CBTC system is introduced in inductive base loop in communication technology that's called signaling system transmission based train control [5]. This system using one advance step of traditional rail system. In this system inductive loop cables was mounted on regular interval of tracks which is coded by certain frequency. Detector is mounted on the benth of train. These detectors reads the specific signal and verified the train location [4]. In 1985 the first inductive CBTC technology system installed in Toronto, Canada in Scarborough RT line Toronto transit commission [2]. In 1983 Lille light metro installing the earlier CBTC of inductive loop based signal and in 1998 first service line is install in Paris line 14 [6,7]. In inductive loop system technology is need around two to three decades but is used nonstandard unshielded wire and cost-effective and easy to install and easy to repair. Due to initial cost is high and risk to theft the conductor. Move to modern CBTC system which is working on frequency range of GHz instead of inductive loop system on KHz [8].

1.9.2 Radio Based CBTC:

As we earlier discussion modern CBTC network working on moving block. This system using Radio communication for high capacity transmission for getting train accurate control information between sideway and train. Getting train accurate information gives a shorter headway and increasing the line capacity. Increasing the line capacity CBTC gives a typical headway of 90 Seconds or less and in Pakistan currently timetable minimum headway is 5minutes and 30seconds [9, 10,]. One more feature in advance CBTC network provide the operator less and undriver train operation [11]. In 2003 first advanced CBTC network on radio based is install in San Francisco airport which is provided by Bombardier [2]. In 2018 First advanced CBTC Network is installed in Lahore Pakistan

1.10 Overview of CBTC:

Widely using a telecommunication in signaling system between the track equipment and train for the infrastructure control and management in railway System is known as CBTC. In CBTC result more accurate efficient, safely to manage and determine the exact location of trains in railway traffic like metros subways for improving better headway and safety. CBTC system include five subsystems, which is Automatic Train Supervision (ATS), Automatic Train Protection (ATP), Automatic Train Operation (ATO), Zone Controller (ZC), and train–ground communication shown in figure 4. CBTC signal system is designed to reduce operational costs, improve train and passenger safety, and increasing train Line capacity. According to IEEE 1474 standard CBTC system provides the continually auto train control process with implementation of Automatic Train Protection ATP further feature is under the automatic Train supervision ATS function. Automatic

Train Operation ATO by utilizing the determination of automatic highly resolution train location under the track circuits, train borne and wayside processer. Increasing population intra city transport need increasing the demand of more safe, fast reliable mass transit system. Subsystem ATS makes the timetable for each train separately. It will be responsible to manage the time between the two stations for each trip. Also ATS include the responsible of passengers comfort or energy saving, Subsystem ATO delivered the guidance optimization trajectory. The trajectory guidance is a velocity profile on distance base, which indicates the optimal velocity a specific position. The main task of the ATO subsystem is to bring the train to this derived guidance trajectory. In CBTC system send and receive bidirectional continually wireless communication between station adapters (SA) in the train and ground Access Point antenna. The railway system line is divide into two areas. Every area has own wireless system of transmission under the control of Zone controller ZC. ZC is controlled the direction, location and velocity of train. ZC is responsible under their area control and make sure the wireless link of each train in all times. Mass transit authority is provides the required time table for run the operation in mainline and Operational Control Center OCC is mange the timetable and send the data to ZC through ATS. ATP is responsible to calculate the all trains braking and traction capabilities according to receiving the data of movement authority. If the train is reaching there velocity the system is automatically apply the brake and emergency brake for protection the each train [14]. The system uses real-time train information, such as train position and speed, to calculate the safe distances between trains and control their movements. On the requirement CBTC provides lowest headway time and increasing the line capacity. Figure 4 illustrate CBTC Component On Board overview.

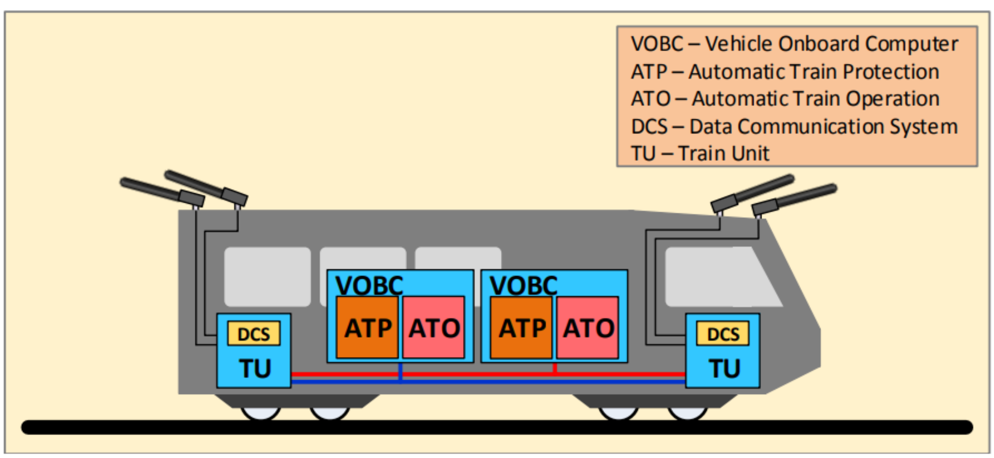

Figure 4: CBTC onboard Component

CBTC Signal System gives us to different type of automation level or Automation Grades Defined as GoA which is discuss in IEC 62290-1. CBTC considered as Basic technology of Driverless trains. Five automation grades which is known as GoAs levels are follows.

GoA automation grade 0, without any type of train, route protection or Called Manual Train operation.

GoA automation grade 1, Train drive apply manually apply traction and brake but under the observation and limits of automatic train protection ATP which is increase the overall system performance and safety.

GoA automation grade 2, in this system the train is under the supervision of automatic train operation ATO automatically apply the brakes and gives the traction need of the operation but driver still in the cabin and control other functions like high voltage air condition settings door opening and closing and many other passenger related functions

GoA automation grade 3, In this level train driver is free to move in the control cabin but still he is exit there for detect and abnormality and presence of hazards it is driverless train operation DTO.

GoA automation grade 4, this level is totally under system observation no need any person in this system it's called Unattended Train Operation UTO [14].

1.13 Radio intrusion Detection:

Illegal access or intrusion with radio signals used in CBTC train communication is called radio intrusion. It can disturb train communication by interfering with the operation of radio signals used in the CBTC train. This misleads the train communication and delays information that controls the train. To protect the train system, a Rail-Radio Intrusion Detection system (R-RIDS) has been developed for CBTC [34]. Radio technologies defined in the railway communication framework for directing the passage of trains and transmitting warnings. Signal characteristics, stops, speed limitations, and track conditions are all represented in the commands and cautions given to the train. The locomotive responds by taking the necessary steps to guarantee safe travel. SDR-based CBTC networks could be the target of cyber security attacks that threaten railway workers or compromise the safe operation of trains by compromising their ability to navigate. To address this issue, the Rail-Radio Intrusion Detection System R-RIDS was developed to identify and prevent cyber attacks such as message tampering, commanding replays, and guessing. For the security of communications between locomotives and beacons, RRIDS is a rail command-specific IDS. Near real-time intrusion detection is carried out via RRIDS [35]. A cyber detection module integrated with an intrusion detection system is used for the classification and detection of cyber attacks, intrusion, and many types of data sale and stalling activities. The system is reliable for host-level network systems and can automatically work on time. Based on intrusion behavior, IDSs differ between host and network base systems. The system is under operation for criminals [36].

1.13.1 Types of IDS

1. Host-based IDS
2. Network base IDS
3. Hybrid Host Base IDS [37]

In this paper, an Orange Line subway Lahore platform is used for simulating train operation. In the network simulation of the platform set, the data for train communication were collected. In this information security field, there are two typical types of datasets for radio intrusion detection: a wireless dataset and a wire dataset. For the wired data network dataset, the CIC-IDS2017 [15] is used in this work. It contains more than 5 million records and has more than 42 features. Most of the records are viewed for a sample and labeled as abnormal or normal data. Furthermore, the abnormal dataset includes 39 attack types, which are categorized into 4 groups. [19]. The wireless data network uses the AWID dataset in this set, and the wireless frame is used as the dataset. There are more than 155 features covering all the field layers. The AWID consists of 16 major kinds of attacks that are further divided into three main categories. These are flood attacks, injection attacks, and impersonation attacks

CHAPTER 2

Literature Review

2.1 CBTC Systems:

In overall world is CBTC consisting on two types of systems on the base of communication.

2.1.1 Train to Wayside communication:

This CBTC system working on train to side-way equipment T2W. In this system command Centre/control Centre send the information to zone level Access point AP antenna of trackside then this information send to relevant train onboard after receiving this information train onboard send this information to nearby access point AP Antennas then this information further proceed to control Centre. This process is repeating again on every single train its called train to wayside communication. Train-to-wayside communication is typically achieved using a wireless communication system, such as Wi-Fi or cellular network, between the onboard equipment and the wayside equipment. The onboard equipment continuously sends and receives data, such as train location, speed, and other relevant parameters, to the wayside equipment. The wayside equipment then uses this data to calculate the appropriate speed and distance commands for each train and sends them back to the onboard equipment. Figure 4 illustrate the train to way side communication.

2.1.2 Train to Train Communication:

CBTC (Communication-Based Train Control) systems, "train to train communication" refers to the communication between trains within the system. This communication is essential for maintaining safe and efficient train operations, coordinating movements, sharing critical information, and ensuring the overall integrity and functionality of the CBTC system. Training for train to train communication involves equipping train operators, control center personnel, and other relevant stakeholders with the skills and understanding necessary to communicate effectively in CBTC environments. This training typically covers aspects such as using communication devices and protocols, interpreting and responding to messages, understanding system limitations, troubleshooting communication issues, and adhering to established procedures and protocols. By providing comprehensive training for train to train communication, individuals and teams can develop the necessary competencies to communicate effectively, mitigate risks, and ensure smooth operations in CBTC systems [18].

2.2 CBTC Network Components:

Train to wayside components on the base of two way communication discus the typical major components of CBTC system. In this section further this system consisting following subsystem [10, 15].

- Train On Board Network
- Train to trackside radio Network
- Track side backbone network

2.2.1 On board Network:

On board network equipment consist of vehicle onboard computer/controller also using the term is carborne controller or onboard control unit OBCU. VOBC/OBCU include further system which is working on the base of onsite situation with ATO system and ATP onboard system [9]. These systems shows the figure …

The onboard is also consist on one major part is a data communication system DCS or e say radio communication system RCS. For all type of communication behind the wayside and train is responsible for radio communication. DCS is a system of VOBC integrated with combination of hardware and software. In hardware included the antennas and Radio. These all system refers to T.U train Unit. Onboard Component show in Figure 4.

2.2.2 Wayside Components:

Wayside is further divided in zones. These zones are responsible to control the all components and in own network control all the train that is called Zone Controller. The fundamental function is improves the network into zone or its own side infrastructure and maintaining the safe zone operation in zone and also help to improve the failure fundamental of the zone and cooperate with nearby zone. This zone also has own ATO and ATP system. The other important thing is wayside and trackside not a general same terminology. Trackside components are consisting on track components like beacons and odometer Access point antennas and wayside consisting on OCC components [2]. The main components is illustrate in Figure 5 of wayside and trackside.

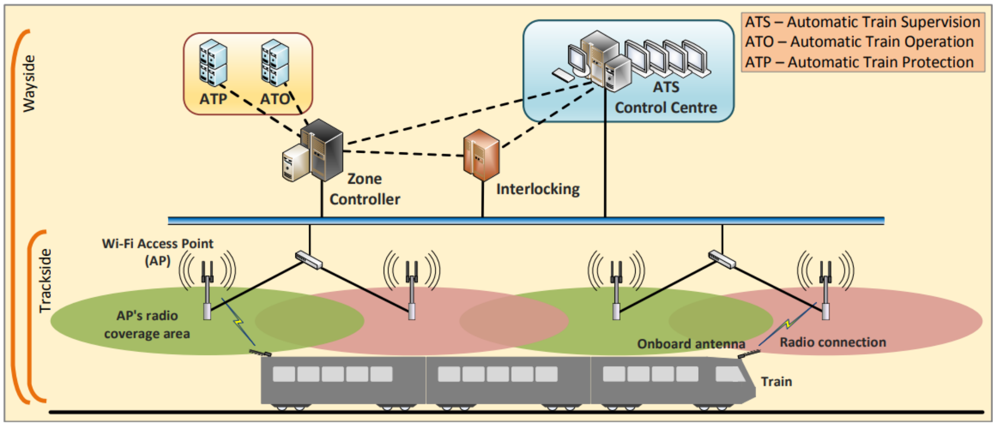

Figure 5. Way Side component

ZC is one main system is ATS which is responsible for scadulaing and maintaining the train on main line on exact time. ZC subsystem ATP is manage its all communication network with in its zone train. This system are responsible to manage all the trains on the instruction of MA movement authority. One ATC subsystem includes the CI computer base interlocking. CI is responsible to setting the train routes and manage the trackside equipment like signals, points and switch machine. The other subsystem of ATO is manage all the trains on its relevant destination with on designated time [9]. Trackside equipment consisting of Wi Fi cell is serving only one AP antenna.

2.2.3 Configuration of Track side network.

On the base of trackside communication it has two configuration in the world.

A traditional trackside network of is consisting on Star topology. Using optical fiber cable infrastructure directly connected to wayside to AP Antenna. In a CBTC system, the star network topology is commonly used for the radio communication between the trains and the wayside equipment. In this configuration, the trains act as the nodes and the base stations or antennas act as the central hub or switch. The base stations communicate with the trains using radio signals, and the hub manages the transmission of data between the trains and the wayside equipment. The star network topology provides several advantages in a CBTC system, including:

- High reliability: The central hub provides redundancy and ensures that communication is maintained even if one or more nodes fail.
- Efficient data transmission: The hub manages the flow of data between the nodes, which can help prevent congestion and ensure that all devices receive the information they need.

- Simplified installation and maintenance: The star topology is relatively easy to install and maintain, making it a popular choice for CBTC systems. [19]

To days consisting network and latest track side network is ring topology.

A ring network in CBTC refers to the physical topology of the communication network used to transmit data between the trains and the control system. In a ring network topology, the communication links form a closed loop, where each node in the network is connected to the two adjacent nodes. In the context of CBTC, this means that the trains and the control system are connected in a closed loop, where each train communicates with the train in front and behind it, as well as with the control system. The ring network in CBTC has several advantages. First, it provides redundancy, meaning that if one link in the network fails, the data can still be transmitted through the other links in the loop. This ensures the reliability and availability of the system. Second, the ring network topology enables high-speed data transmission and low latency, which is critical for real-time train control. Overall, the ring network topology is a popular choice for CBTC systems because of its reliability and efficiency in transmitting data. Difference is illustrate in Figure 6[20].

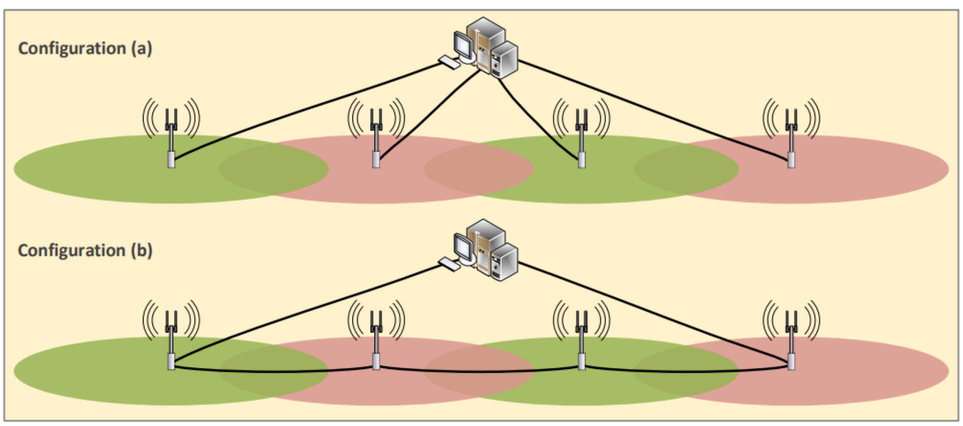

Figure 6. Star topology and Ring topology

Railways are a crucial component of the nation’s infrastructure because they transport people and goods from one place to another. The railway system is complicated, geographically scattered, and increasingly reliant on information and communications technology (ICT), just like other essential infrastructures. As a result, reducing ICT risks is crucial for safeguarding the railway infrastructure. Information and communications technology (ICT)-based systems are vulnerable to errors and flaws that can be deliberately exploited. Because of the significance of these infrastructures to business, government, and society as a whole, the application of ICT to them creates major security concerns. The European Commission and the US Department of Homeland Security both classify railways as a key infrastructure in the transportation industry. Due to their responsibility for both the transportation of people and products, railways are essential to a country's economy [17].

In this smart, era there is a need to improve and make the system efficient by introducing the latest technologies in the railway system. The traditional railway system, which only has a half-century of experience, uses axle counters and track circuits to locate trains using the signal system. The number of unplanned delays and train accidents is currently increasing daily. This is the main driver behind the need to switch from traditional railway systems to modern ones around the world [18].

Concerns have been raised among a variety of new and existing users about RF interference between CBTC-equipped trains due to the growing development of CBTC by public transportation agencies that employ a data communications system based in the 2.4 GHz ISM band. The proliferation of "Wi-Fi" hotspots, wireless computers enabling untethered internet access by the general public, and RF identification (RFID) technology have recently added to the vast number of RF devices that currently operate in this band (like microwave ovens, medical devices, cordless telephones, etc.). The main source of concern is the band's popularity, ironically this popularity harvests many benefits and advantages to the CBTC system that uses it. Heavily used frequency band proximately prevents its use for those systems that consider themselves mission critical. Although it is a wise line of action to avoid a frequently used frequency band for an essential application, it might not be practicable or, upon closer inspection, even necessary. The expense and technical risk of gaining a regulatory license or constructing the special radio equipment might prove to be unaffordable, or there could not be any alternative spectrum available. Furthermore, any apparent interference may be fully eliminated by technological advancements in radio equipment and signal processing [19].

The old Track-Based Train Control (TBTC) system's capacity and safety have been proposed to be improved by the communication-based train control (CBTC) system. According to past studies, railway line capacity and safety have been boosted by the continuous wireless connection provided by the CBTC system. The operating conditions, such as the time delay between subsequent trains, the ratio of rapid to slow trains, communication ambiguity, and positioning system accuracy, are substantially correlated with these improvements. It is necessary to compare the performance of the TBTC and CBTC systems since the benefits of implementing the CBTC system might alter depending on the operating circumstances [20].

A presented the experimental findings defining the working and effectiveness of RRIDS against a hypothetical attacker. The control systems of different countries such as the European traffic management system, advanced civil speed enforcement system II and interoperable electronic management system of the USA use communication-based control and future Software Defined Radio (SDR) technologies in the communication framework for directing the passage of trains and transmitting warnings. Signal characteristics, stops, speed limitations, and track conditions are all represented in the commands and cautions given to the train. The locomotive responds by taking the necessary steps to guarantee safe travel. SDR-based CBTC networks could be the target of cyber security attacks that threaten railway workers or compromise the safe operation of trains by compromising their ability to navigate. To address this issue, the Rail Radio Intrusion Detection System (RRIDS) was developed to identify and prevent cyber-attacks such as message tampering, command replay, and guessing. For the security of communications between locomotives and beacons, RRIDS is a rail command-specific IDS. Near real-time intrusion detection is carried out via RRIDS [21].

These are flood attacks, injection attacks, and impersonation attacks.

Table No 2. Technical Challenges in Railways and Their Proposed Solutions

Issues in CBTC network	Challenge in network	Purposed solution	Ref.
DoS system detection	some small variable changes in train network traffic flow and its difficulties to detect.	• Using some sequential techniques for analysis Results	22
DIA-detection	Old available detection model can only and hardly identify DIA attack.	• In depth analysis of CBTC network protocols. • check authentic of LMAs	23
Distinguish of CBTC attacks in faults	Faults are the same impact on attacks do.	Adding a detection model based on device states. • Designing an HMM classifier.	24

Train ground communication system	Intrusion comes in communication Train Ground	Add a modal base on Adda Boost Classifier	26
Purposed base cyber intrusion detection	Jammer single brakes and take Emergency Brake	Adding a new detection modal base on M-Gram Modal on Gradient boost Classifier	Purposed Work

studied that over the past ten years Modern, communication-based signaling systems have significantly replaced outdated, railway-specific signaling systems. With more than a hundred systems now installed worldwide, CBTC is the preferred technology among mass-transit train operators today. Applications that are safety-related and time-sensitive, like train control, place strict constraints on the radio communication technology utilized. Despite being designed initially for stationary users in a small area, IEEE 802.11 Wi-Fi has become the standard radio technology for CBTC. Unfortunately, because of the intense competition in the railway sector, there is virtually little publicly accessible literature on this subject. The security and accuracy of the signaling system are linked to both the life safety of the passengers as well as the security and effectiveness of the rail transit operation. Obtaining the safety certificate for the trial operation with transporting passengers is necessary to ensure the security of a signaling system for the metro [22].

Positive train separation, over speed protection, and worker safety are all provided by communications-based train control (CBTC). Because trust management solutions are not already incorporated into system designs, CBTC transmissions are vulnerable to attackers. To identify unique CBTC system vulnerabilities and the necessary system security measures, the architecture of CBTC systems as well as conventional train control methods are analyzed. The proper trust management system is then derived using the security requirements. The influence of these trust management systems on permitted traffic delays and system velocity, or how they relate to train dynamics, have not been taken into account in the existing work on safe cross-domain dispatch operations. To provide engineering estimations of the viability of potential trust management systems to support rail operations while minimizing collisions, a link between train dynamics and trust management delay is presented. There is a specified algorithm for the safe and secure scheduling of trains through the interchange point. In the worst-case traffic scenario, the algorithm offers positive train separation, allowing for safe and secure scheduling while minimizing traffic delays. The method is explained with the help of an example and is not dependent on any particular security management, CBTC, or dispatch system [23].

The radio system is the first over-the-air (OTA) wireless technology implementation in a revenue-generating urban rail transit system. The system has worked flawlessly and is proof that advanced technology can be applied to difficult situations. The Ethernet 802.3 open standard is the foundation of the complete data communications system (DCS) supporting the CBTC. The 802.11 mobile network expansion of this standard is used in the radio section. Because it has the best resistance to interference and offers more than sufficient data rates, the 802.11 frequency hopping spread spectrum (FHSS) variation is employed. The 802.11 standards have been applied for mobile networks capable of routine hand-overs between access points at up to 100 km/h, and the entire network was developed and constructed using technology that is readily available commercially. The system design used the 2.4 GHz ISM band standard to achieve flawless performance and entailed multiple intricate steps. Before designing the network to handle this data, it is necessary to comprehend the nature of CBTC data. Next, link budgets must be established in light of the monorail's particular guide way environment. Signal strength surveys were carried out to determine where to place access points such that there was full and redundant coverage throughout the guide way. Furthermore, severe co-user interference (802.11b or Wi-Fi) is present at several locations along the guide way and had to be accommodated. Finally, the operating parameters of the radios had to be fully understood to optimize the handover process. The complete system was extensively tested and many weeks of data were collected to verify that the radio system met the performance requirements. Keywords: radio CBTC, ATC, driverless, monorail [24].

Kola S. et al., (2018) presented that American railroads plan to complete the implementation of their positive train control (PTC) systems by 2020, with the primary safety objectives of avoiding interbrain collisions/train derailments and ensuring railroad worker safety. Under published Interoperable Electronic Train Management System (I-ETMS) specifications, the onboard unit (OBU) communicates with two networks: 1) the signaling network that conveys track warrants to occupy blocks, and 2) the wayside interface unit (WIU) network, a sensor network situated on tracks to gather navigational information. These include the status of the rail infrastructure (such as switches) and any operational hazards that may affect the intended train path.

Due to several advantages, for instance, lower maintenance cost, and improved driving headway, the Communication-based Train Control (CBTC) system, the modern train control technology, has been extensively useful throughout the world. Through real-time train tracking, the technical foundation of CBTC is to guarantee a safe distance between trains. Since 2010, the Korean CBTC standard known as the Korean Radio-based Train Control System (KRTCS) has been established. The KRTCS system consists of automatic train supervision (ATS), roadside/onboard automatic train protection (ATP), automatic train operation (ATO) onboard, electronic interlocking (EI), and wayside equipment such transponder tags, precise stop makers, communication networks, etc. [25].

The efficiency and security of the urban rail transit system have been improved by the application of communication-based train control technologies. Amounts of possible security vulnerabilities are created in CBTC systems with the rise in informatization and automation through the use of communication, computer, and control technologies, where hostile attacks might be executed. Traditional intrusion detection systems (IDS) are ineffective at detecting some assaults, such as data manipulation operations, which can have an impact on the safe functioning of CBTC systems, such as rear-end collisions. The paper first proposes a model to measure the effects of data tampering attacks on trains based on the operating principles and information exchange characteristics of CBTC systems, and an intrusion detection method is developed based on the running status of the train through the Kalman filter and 2 detectors. The technique enhances the 2-detector's ability to recognize data tampering attempts and to constantly emit alerts throughout the assault. The enhanced approach offers a decreased false negative rate and more accuracy [26].

All over the world, the most reasonable convenient, and popular way of transport is by railway. It is a comfortable mode of transport. Most of the train Accidents are occurs due to human negligence [57]. Due to the high speed of trains which takes time to control, it becomes difficult to avoid train accidents. There is a need to introduce an efficient system to identify the problem of train collisions and send the report to the operator or control room before a collision occurs. To avoid the train collision still, there is no solution. Many countries have developed solutions based on Anti-Collision Device (ACD) systems. For convenient reading by surveillance system inside the locomotive, the train tracks in the railway are divided into smaller frames each having a 10 km distance, each track given with a specific track number. As a result, the railway track requires the track ID to be provided every 10 km. As a result, the railway track requires the track ID to be provided every 10 km. By using Radio Frequency Communication, the tracking number is shared with the base station. To take proper action system sends an SMS through the GSM network to the official person, if two trains are traveling on the same track. The system avoids collision by using RF Module in areas where the GSM network is poor. If an obstruction is seen anywhere there is a crossing, the LDR sensor and microcontroller unit respond appropriately [27].

Human carelessness and human error have become the main cause of train accidents all over the world. The automated surveillance system is the main feature of each locomotive. The railway network's train tracks are divided up and given unique track numbers that a locomotive's surveillance system can read. The surveillance system will use radio frequency communication to relay this tracking number to nearby trains. Track numbers are compared with neighbor track numbers by the system. When the monitoring system detects similar track numbers, it takes action to notify the worried motorman so that he can stop the train and avoid accidents. Additionally, a communication protocol is provided to ensure data flow among the half-duplex mode devices' radio frequency transceivers [28].

The main purpose of the train control system is automatic train protection, which reduces speed and applies brakes to assist avoid crashes. To increase the system's applicability in the commercial sector, safety study and assessment of autonomous train protection using simulation are necessary [29].

A supervisor mode of patrol inspection based on radio frequency identification (RFID) and information management technologies to promote standardization, control the level of railway track inspection, and monitor inspectors scientifically and precisely. The portable data acquisition devices (palm and reader) and terminal systems used for data management make up the railway track inspection system, which is installed on electric poles or milestones. One of the important practical applications of this system contributes to improving the reliability of railway track inspection, preventing equipment accidents, and ensuring travel safety by reducing the workload of patrol inspection, increasing the ratio of arriving at designated locations during patrol inspection, and providing reliable information for the management of railway equipment's drawbacks. [30].

One of the potential wireless communication technologies in the railway sector is the use of RFID. Numerous RFID railway applications are in the early stages of development in various regions of the world. These include train positioning and location, operation and upkeep, measurement of the temperature of the train axles, track inspection system, wagon monitoring system, etc. RFID implementation automates a vast and intricate train network. Thus, the use of RFID technology may significantly increase operational effectiveness, assure human and machine safety, and minimize financial losses [31].

Despite being widely utilized in many fields, Radio Frequency Identification (RFID) still needs to have its standardization, anti-collision algorithm, and system measurement accuracy improved. The author also highlights the development trend of RFID technology in our nation through an overall analysis of global manufacturers' use and study of RFID technology [32].

Numerous fixed and moving items have been tracked and identified with the use of RFID technology. The enhancement of large-scale transportation infrastructure's dependability, timing, and efficiency is one of the most difficult RFID applications. For instance, one of the many technologies now being used in China to monitor and manage the railway system is Radio Frequency Identification (RFID) technology in UHF frequencies (840-845MHz and 920-925MHz). Despite the ATIS RFID-based system's excellent performance for conventional trains traveling at up to 150 kph, several issues must be fixed before this technology can be applied to contemporary high-speed and ultra-high-speed railway lines operating at up to 500 kph.[33].

Using RFID tags allowed for the creation of a real-time container track, integration of information flow and physical distribution, and the container acting as a carrier of information flow. When a train arrives at a station, the railroad’s bureau's database can obtain precise information on the approaching train thanks to the ATIS System. [34].

1. Communication-based train control (CBTC) is a computerized train control system to guarantee safe train operation using communication technologies [40]. The utilization of railway infrastructure can be enhanced by a communication-based control system, to provide the people with better services. Computer-based control systems are distinctive cyber-physical systems (CPS) that connect the control of the physical world with the computing and communication of the cyber world. The substantial use of computer, communication, and control technology in CBTC has

greatly increased the system's level of automation while also putting it at risk for cyber-attacks [35].

Cyber security incidents in the railway system have increased over the last few years. By targeting the station fire systems in November 2016, in San Francisco hackers took over the metro train [42]. This attack damaged about 2112 computers. Danish state rail operators experienced extraordinarily widespread denial of service assaults in 2018. On Sunday, ticket sales were suspended throughout the nation [36]. Cyber-attacks might cause an emergency brake and have a significant impact on the amount of time passengers take to travel since CBTC systems are considered critical to safety [56].

To detect cyber-attacks over the system intrusion detection system are organized. It keeps an eye on the system for unusual activity and policy infractions so that the proper action may be taken right away [37]. The construction of an Intrusion detection system for CBTC is a practical solution to raise the level of security protection. Therefore, CBTC systems must conduct a thorough and in-depth investigation of the intrusion detection problem. Traditional IDSs have not been designed with the characteristics of CBTC in mind. Additionally, assaults are likely to activate the CBTC systems' fault-safety mechanism. They could be mistaken for other defects like equipment malfunctions or communication breakdowns. Traditional IDSs cannot differentiate between defects and cyber-attacks because they may have an identical effect on CBTC systems as cyber-attacks do [38]. They will decrease the effectiveness of the IDS and result in false -ve or false +ve.

Introduction to intrusion detection

Presently, intrusion detection is a crucial security technique. It may be divided into two categories: anomaly-based detection and signature-based detection [39]. To detect the attack signature based depends on static signatures, it is incapable to identify mysterious cyber-attacks. Another method which is anomaly-based recognizes the attacks by spotting an eccentricity from expected behavior. The ability of the anomaly-based IDS to identify previously undisclosed "zero days" attacks has drawn the interest of an increasing number of researchers. The anomaly-based CPS techniques may be divided into machine learning, statistical-based, and related rule-mining algorithms [39].

For more than 25 years, passenger transport has been reliably and securely provided by Communications Based Train Control (CBTC) signaling systems. CBTC, which was formerly seen as a futuristic novelty in technology, is today recognized as the most recent iteration of standard transit system control. But there are some expenses to understand. Whatever the driving force, once the decision to upgrade to CBTC has been taken and the scope of the upgrade has been established, the implementation must be meticulously planned and carried out to minimize the impact on continuing operations and to guarantee safety throughout the upgrade process [54]. This standard specifies the performance and functional criteria for a communications-based train control (CBTC) system. Continuous, high-capacity, bidirectional train-to-wayside data communications; train-stood and wayside processors capable of executing automatic train protection (ATP) functions; and optional automatic train operation (ATO) and automatic train supervision (ATS) functions are all components of a continuous, automatic train control system, or CBTC. This standard specifies headway standards, system safety standards, and system accessibility criteria for a CBTC system in addition to CBTC functional requirements. The whole range of transit applications, including automated people movers, are covered by this standard [40].

To find assaults, the rule-based IDS examines whether events happen in a sequence. To determine whether the system is being attacked by hackers, it unearths the relationships between the traits of the data set. Using the related rule mining approach, Yang creates an IDS for SCADA systems (supervisory control and data acquisition). The IDS can do a deep protocol analysis and a deep packet inspection. Traditional IDSs are unable to keep track of physical behaviors, but Koyena uses association rule mining to evaluate sensor and actuator data to find new attacks. Additionally, the majority of rule-mining algorithms cannot handle continuous attributes. The innovative approach can considerably lower false alarm rates in the medical CPS [41]. In the statistically based intrusion detection approach, rare events are viewed as anomalies. Statistical models for anomaly detection have been designed using both parametric and non-parametric methods. Both parametric and non-parametric techniques have been applied to design statistical models for anomaly detection. When used in non-stationary systems, parametric approaches that estimate the parameters from the provided data may produce inaccurate findings [42]. Non-parametric approaches are employed to solve the issue since they can accurately alert users to aberrant activity and quickly identify DoS assaults. When the intensity of the anomalous traffic is less than 5% of the background traffic, the detection rate is, nonetheless, poor. To attain a high detection rate and a low misclassification rate, Manikopoulos offers a multi-window statistical technique utilizing statistical modeling and neural network classification [43].

Wireless local area networks (WLANs) are used by communication-based train control (CBTC) systems to communicate train status information and control instructions. Random transmission delays and packet dropouts are unavoidable with WLANs since they were not initially intended for applications requiring high levels of mobility. As a result, trains may need to brake unnecessarily or even in an emergency, which reduces line capacity and decreases passenger pleasure. In this article, we examine how random packet drops affect the stability and performance of CBTC systems, analyze the effects of random packet drops on those systems' handovers and transmission errors, and offer two innovative techniques to boost those systems' performance. We perfect the system to switch a group of trains as a networked control system (NCS) with packet losses in transmissions, in contrast to prior studies that only take into account a single train and analyze the communication difficulties and train control issues individually. The outcomes of extensive field tests and simulations are given [54]. We demonstrate that, when compared to the current scheme, our suggested solutions may offer lower energy use, greater ride comfort, and larger queue capacity. A CBTC system is made up of both physical and digital processes. Data communication systems (DCS), onboard equipment, and roadside equipment make up a typical CBTC system. The cable backbone network connects the wayside equipment, such as the automated train supervision (ATS), zone controller (ZC), computer interlocking (CI), and data storage unit (DSU). The cable backbone network connects the wayside equipment, such as the automated train supervision (ATS), zone controller (ZC), computer interlocking (CI), and data storage unit (DSU). The onboard equipment, also known as the vehicle onboard controller (VOBC), includes the wayside equipment, automated train protection (ATP), automatic train operation (ATO), and mobile station (MS), which connects with the onboard equipment over the wireless network. Equipment that is redundant and fault-tolerant is used because CBTC systems have strict reliability and safety requirements [44]. For data transfer, redundant networks and specialized secure communication protocols are used. In a CBTC system, ZC receives the location and speed of the preceding train over the wireless network. ZC creates and communicates the limitation of the movement authority (LMA), a point on the line that the train cannot pass, to the next train after receiving the information from the prior train and the information on the safe path from CI[53].

Cyber attacks' Effects on CBTC Systems The conventional rail system utilizes a track-based train control (TBTC) technology that transmits data through track circuits [45]. Track circuits are used in traditional track-based control systems to transmit information. Since TBTC is physically cut off from outside networks, cyber security concerns are not taken into account. CBTC systems are widely used across the world as urban rail transport systems carry a rising number of passengers. CBTC systems make substantial use of commercially available (COTS) goods, such as common computers, commercial operating systems, common communication protocols, etc. COTS increases the system's level of automation, reduces the time between trains, and increases the capacity of urban rail transportation, but at the same time, it increases the danger of cyber-attacks [46]. When the CBTC systems are functioning properly, the ATP of the subsequent train determines the protective position/speed curve using the LMA that was received. The next train's ATO computes a service braking curve beneath the ATP curve and directs the train to follow that curve. To do this, cyber-attacks can directly or indirectly compromise the LMAs' availability or integrity. Due to packet loss and delay brought on by faulty wireless communications, designing some train control systems through train-wayside communications is a difficult issue [47].

For multigrain CBTC systems with packet delay and loss, a networked control system (NCS) model is developed. Then, to improve the service quality provided by CBTC systems, we suggest a revolutionary train control technique. Retry limit adaptation in the medium access control layer and guiding trajectory update are employed in the suggested approach to reduce energy consumption and trip time tracking errors, respectively. The suggested technique can significantly enhance the service quality of CBTC systems, according to extensive simulation findings. Both static and time-varying wireless settings can minimize energy usage and trip time inaccuracy [48].

Wireless networks, such as wireless local area networks (WLANs), are used in communication-based train control (CBTC) to broadcast directives and train status. As the train control system (TCS) depends on precise, timely, and reliable data across communication lines, CBTC systems have strict criteria for train-ground communications. Although random packet delays and losses are unavoidable in WLAN-based CBTC systems since WLANs were not initially intended for high mobility environments, this might lead to excessive train traction, braking, or even emergency braking, as well as decreased line capacity and passenger pleasure[52]. We take into account a group of trains in CBTC systems as opposed to prior efforts that just take into account one train to enhance CBTC performance. The outcomes of extensive field tests and simulations are given. We demonstrate that growing the distance between trains in a stable state, which results in increased cost of line capacity, is necessary for the existing control strategy in CBTC systems to maintain stability and performance during transmission delays. Our suggested plan, however, has the potential to greatly raise CBTC performance. [49]

Due to certain environments, including tunnels, the use of wireless technology for public transit may entail several restrictions. Consideration is given to the signal attenuation unique to tunnel propagation. To reduce connectivity loss while the train switches between Access Points, we suggest optimizing the changeover detection system. We suggest a performance assessment using the OPNET simulator [50]. CBTC (communication-based train control) has replaced other automatic train control systems as the primary one as a result of advancements in electronic communication technologies. The United States traveling public as a whole will profit greatly from high-speed rail operations in the regions they serve. GSM-R, a specialized version of the GSM procedure used for cellular telephony, is utilized by high-speed trains in Europe and Asia. The European Rail Traffic Management System (ERTMS) is a unified Communications-Based Train Control (CBTC) system that is supported by GSM-R. In addition to being deployed in China and India, ERTMS provides high-speed train services throughout Europe (1). There are plans to build a high-speed rail track between Boston and Washington, D.C., along the West Coast of the United States. Using their E-VTMS (Enhanced Vessel Traffic Management System) (2), which was created by BNSF, Class-one freight railroad companies (BNSF, NS, CSX, and UP) and the primary high-speed passenger railroad company, Amtrak, are working together to provide a consistent Communication-Based Train Control (CBTC) system. The 220MHz frequency band [217–219MHz for the uplink and 221-222MHz for the downlink] is used by American railways for rail signaling [51].

At the end of this chapter we can try to overcome the intrusion in CBTC network. In further chapter design a algorithm for intrusion detection.

Chapter 3

Methodology

In chapter 3 discuss the intrusion in CBTC network and also we will find method on intrusion detection. How implement a new machine learning technique to find the intrusion and method of implementation. The author of this work is also belongs to CBTC network project called OLMRTS Lahore. As his observation when any jammer is going through near the line train is stop in emergency brake and DMI dynamic machine interface shows RAD icon its mean radio communication failed after a few second emergency brake released and speed code available in normally that's way first discus the attack Types

3.1 Attack type of CBTC system

The CBTC attack is totally different from other IT services network attacks because in industrial control system is working on application of applied private protocols. This protocols contain on systematic packet opening and reverse parsing protocol technology. Second industrial program using months, years without stop and kept steady operation that's way without any interruption it is very different to reboots or updating. On the other hand CBTC intrusion attack is totally different and based on communication and further divided into two type's data spoofing attack and denial of servicing [52]. In this system DoS attack preventing the CBTC data to exchange the integrity for exploiting the of devices. Normally DoS attack is two Type. One is violent attack is various forms like Physical damage to infrastructure, Cyber security breach, Unauthorized access or intrusion, Threats or violence towards personnel.

It's important to note that CBTC systems are designed with multiple layers of security measures to mitigate potential risks and ensure safe and reliable train operations. These security measures include encryption protocols, access control mechanisms, firewalls, intrusion detection systems, and cyber security protocols. In a semantic attack, an attacker may manipulate or exploit the semantics of the data or commands exchanged between different components of the CBTC system. By doing so, they can attempt to deceive or mislead the system, causing it to behave in unintended and potentially harmful ways. And the second is Semantic attacks can undermine the integrity, reliability, and security of the CBTC system. They require a deep understanding of the system's protocols, data structures, and semantic rules to effectively exploit the vulnerabilities. To mitigate semantic attacks, CBTC networks typically employ various security measures such as encryption, authentication, access controls, and anomaly detection systems. Regular security assessments, updates, and vigilant monitoring are also essential to ensure the system's resilience against potential semantic attacks. Attack type table are below.

Table 1. Attack Type

No	Attack types	Description	Attribution
1	Beacon Flood	Forge a large number of beacon frames to make the terminals unable to access the correct AP (access point)	DoS
2	Probe Request Flood	Forge a large number of probe request frames to consume legitimate AP resources	DoS
3	Probe Response Flood	Forge a large number of probe response frames to affect station access networks	DoS
4	Authentication Flood	Forge a large number of authentication frames to break the connection between the legitimate user and the AP	DoS
5	Association Flood	Forge a large number of association frames to break the connection between the legitimate user and the AP	DoS
6	Deauthentication Flood	Forge a large number of deauthentication frames to break the connection between the legitimate user and the AP	DoS
7	Deassociation Flood	Forge a large number of deassociation frames to break the connection between the legitimate user and the AP	DoS
8	RTS Flood	Forge RTS frames with a large Duration value to block the wireless channels	DoS
9	CTS FLood	The fake legal node sends a large number of CTS frames to cause other nodes to stop sending data.	DoS
10	Man in the middle Attack	Intercept and falsify the normal communication data between the legitimate user and AP.	Data spoofing attack
11	UDP Flood	Attack train ground communication system AP through the wired network	DoS
12	ICMP Flood	Make the network channel be blocked by flow among backbone network switch, ZC and AP	DoS
13	TCP/SYN Flood	Attack train ground communication system AP through the wired network	DoS

3.2 Selection of Antenna

This paper discusses the AP Antenna because the CBTC system uses an AP Antenna and attacks the AP and damages the CBTC single system

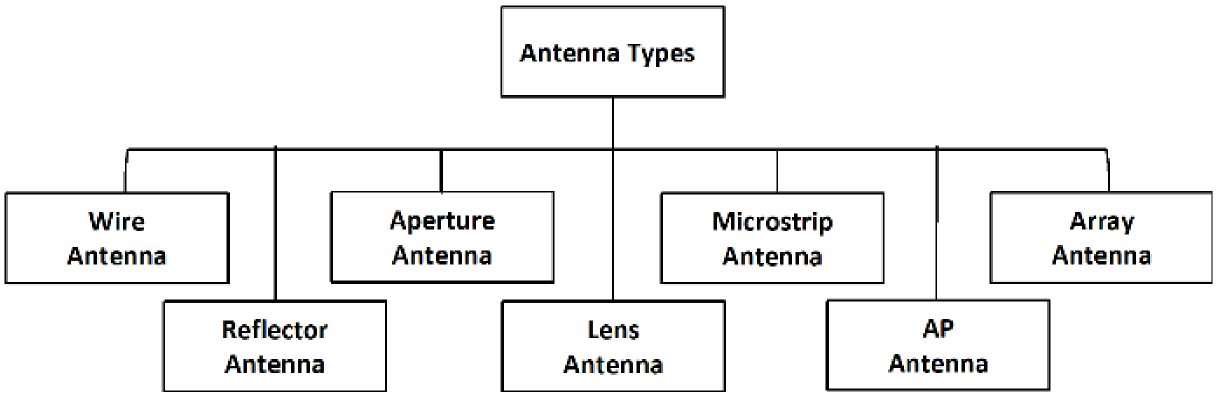

Figure 7. Types of Antennas

In Equation 1 the antenna gain is considered an antenna efficiency, which is determined by the antenna signal capture capacity [23]. The distance R is the input power P_o, which is written as $S = RP_o$. This equation represents that the signal is equal in all directions, and the density power is S, which is Area Sphere $4\pi R^2$. It is 100% efficient [24].

$$S = \frac{G\,P_\circ}{4\pi R^2} = \left(\frac{|E|^2}{\eta}\right) \qquad (1)$$

Also gain is directing achieved the radiation in part of sphere radiation. As the pattern of antenna based again

$$\text{Density in Power } S\,(\phi, \Theta) = \frac{G\,P_\circ(\phi,\Theta)}{4\pi\,R^2} \qquad (2)$$

$$\text{Radiation density } U(\phi, \Theta) = \frac{G\,P_\circ\,(\phi,\ \Theta)}{4\pi\,R^2} \qquad (3)$$

The antenna efficiency is an integral of the surface intensity radiation divided by the input power P_o of the antenna efficiency [25].

$$\frac{P_r}{P_t} = \int_0^{2\pi}\int_0^{\pi}\frac{G(\theta,\varphi)}{4\pi}\sin\theta d\theta d\varphi = \eta e \qquad (4)$$

P_t is represented the integral of sphere radiation and antenna efficiencies is measured by divided of antenna power and radiation power of antenna. And P_r is donated by power radiation.

The effective area is the passing wave of the capture power and terminal delivery power. Delivered to product. Capture power of antenna is passing the waves first then deliver to the nearly same terminal. Given the Area effective of the antenna and incident wave of density. Antenna includes the flat plate array, horn, effective area and parabolic reflector are considered the efficiency aperture and the losses of mismatch, material, distribution ratio of physical and effective area. And the reflector is 55% parabolic.

Directivity is related to the maximum direction and radiation.

$$\text{Directivity} = \frac{\text{maximum radiation intensity}}{\text{average radiation intensity}} = \frac{U_m}{U_o} \quad (5)$$

Efficiency is only depended on directivity and gain, Gain – is measured in efficiency directivity times, and the 4π is divided by intensity radiation in steradians sphere.

The average radiation intensity is [26]

$$U_o = \frac{1}{4}\pi \int_0^{2\pi} \int_0^{\pi} U(\theta, \varphi) \sin\theta d\theta d\varphi \qquad (6)$$

Directivity is expressed in direction of arbitrary $D(\theta, \varphi)$ divided by the radiation average intensity. One of the ratios is the particular direction and power gain

$$D = \frac{4\pi A_r}{\lambda^2} \qquad (7)$$

$$D = \frac{4\pi}{\Omega_p} \qquad (8)$$

The **Ω**p in the degree beam width.

When the antenna is connected to a receiver with an analyzer spectrum then field strength is measured by an RF voltmeter with E strength. With a load resister, the ZL antenna impedance AF antenna factor equals the Ei voltage V rec

$$AF = \frac{E_i}{V_{ee}} = \frac{2}{h} \qquad (9)$$

The unit meter is -1, often given in dB (m-1) [25].

$$\frac{Pd}{P_t} = \frac{A_2 G_1(\Theta,\phi)}{4\pi R^2} \qquad (10)$$

AP Antenna Parameter with Maximum power transfer theorem

If the load impedance is equal to the source impendence, then it is [27]

For the power receiving equation

$$Pr = \frac{P_t \lambda^2 G_t G_r}{4\pi r^2} \qquad (11)$$

Antenna Receiving power Pr

Antenna transmission power P_t

Antenna Receiving Gain G_r

Antenna Transmitted Gain G_t

3.3 Double Band Antenna

A double band antenna is used to receive and transmit signals at the same time. This antenna has two zones, red and blue sections. When a train enters the red zone section, the train's first AP antenna has the strongest capacity in the red zone, and the capacity in the blue zone is weak against the last track side antenna. Going toward the red zone area is weak, and the Train 2nd AP connects weakly strongly with blue and red. The 700 MHz [28] range of this 4-MHz substrate is 679.5 to 758.8 MHz, the band width in the 100 MHz range is 2265 to 2644 MHz [29], and the gain is 9 dB [27].

Antenna configuration.

According to configuration a uni directional antenna provides only in specific area configuration which is transmit signal in narrow coverage area on the other hand the omni directional antenna gives a wide coverage network in almost all direction. To this CBTC solutions varies across these types of antennas.

I. Track side antenna
II. Onboard antenna

Working on track side antenna this work set some parameters

$$Wf = \left(\frac{8e^{A}}{e^{A}-1}\right) \times \mathrm{h} \qquad (12)$$

Where $$A = \left(\frac{Z_o}{30}\right)\left(\frac{\varepsilon_r+2}{1}\right) + \left(\frac{\varepsilon_r-2}{\varepsilon_r+2}\right)\left[0.24 + \frac{0.12}{\varepsilon_r}\right] \qquad (13)$$

For terms W is width, h is height f is frequency

And $Z_o =$ impedance input

$\varepsilon_r = Reletive\ of\ medium\ permitivity$

$$\lambda g = \frac{\lambda_o}{\sqrt{\varepsilon_{reff}}} \tag{14}$$

$$\lambda_o = \frac{c}{f_r} \tag{15}$$

where $c = 3 \times 10^8$

$f_r =$ Antenna resonance Frequency

$\mathcal{E}reff =$ Efectivily free space of premitivly relative

$$\mathcal{E}reff = \left(\frac{\varepsilon_r+2}{4}\right) + \left(\frac{\varepsilon_r-2}{4}\right)\left[2 + 24\frac{h}{Wf}\right] - 1 \tag{16}$$

Feed length in (mm) which is describe in eq 17.

$$Lf = \frac{\lambda g}{4} \tag{17}$$

Table No 1. Frequency bands for antenna use in railway communications technology.

Technology	Frequency	Application
LTE in railway network [29-32]	700 MHz	Long Range Communication
LTE network [30,33]	2100 MHz	Mid-Range Communication
5G network [30, 34]	Sub6 GHz - 28 GHz	High Speed Communication and Ultra High-speed Communication

3.4 Radio intrusion detection

Illegal access or intrusion with radio signals used in CBTC train communication is called radio intrusion. It can disturb train communication by interfering with the operation of radio signals used in the CBTC train. This misleads the train communication and delays information that controls the train. To protect the train system, a Rail-Radio Intrusion Detection system (R-RIDS) has been developed for CBTC [34]. Radio technologies defined in the railway communication framework for directing the passage of trains and transmitting warnings. Signal characteristics, stops, speed limitations, and track conditions are all represented in the commands and cautions given to the train. The locomotive responds by taking the necessary steps to guarantee safe travel. SDR-based CBTC networks could be the target of cyber security attacks that threaten railway workers or compromise the safe operation of trains by compromising their ability to navigate. To address this issue, the Rail-Radio Intrusion Detection System R-RIDS was developed to identify and prevent cyber attacks such as message tampering, commanding replays, and guessing. For the security of communications between locomotives and beacons, RRIDS is a rail command-specific IDS. Near real-time intrusion detection is carried out via RRIDS [35]. A cyber detection module integrated with an intrusion detection system is used for the classification and detection of cyber attacks, intrusion, and many types of data sale and stalling activities. The system is reliable for host-level network systems and can automatically work on time. Based on intrusion behavior, IDSs differ between host and network base systems. The system is under operation for criminals [36].

3.4.1 Types of IDS

4. Host-based IDS
5. Network base IDS
6. Hybrid Host Base IDS [37]

In this paper, an Orange Line subway Lahore platform is used for simulating train operation. In the network simulation of the platform set, the data for train communication were collected. In this information security field, there are two typical types of datasets for radio intrusion detection: a wireless dataset and a wire dataset. For the wired data network dataset, the CIC-IDS2017 [15] is used in this work. It contains more than 5 million records and has more than 42 features. Most of the records are viewed for a sample and labeled as abnormal or normal data. Furthermore, the abnormal dataset includes 39 attack types, which are categorized into 4 groups. [19]. The wireless data network uses the AWID dataset in this set, and the wireless frame is used as the dataset. There are more than 155 features covering all the field layers. The AWID consists of 16 major kinds of attacks that are further divided into three main categories. These are flood attacks, injection attacks, and impersonation attacks.

3.4.2 Tools in Intrusion Detection

In general, the public can perform intrusion detection when administrator objects vary in terms of safety, which is considered here [38].

Kismet. Intrusion detection, which is a benchmark in mobile inside, arranges the packet load and widens the gateway [39].

Frag Route. Forwarding device used for bundle division, which is the protocol of the internet direction of the attacker's frag router. In this process, a broken packet party will be processed [39].

Snort. Freely accessible computer programs, which are defined by congestion language, are generally used. This computer is adjustable [39].

Honeyd. By using a hardware network moderator in network host utilization on various demand location supports on a network with computer calculations [36],

OSSEC-HIDS. It is a famous security that is available openly with the help of free computer programming access. The delivery OS establishes a system between the client and users [37].

In Fig. 6, the module extractor features and the main data capture source module for data storage use the generation of the database from the wireless and wired-on-ground train communication system, and this database includes all types of abnormal data and all types of normal data. The module data for capture are from the first capture and the wireless dataset IEEE-802.11 for the train ground system communication system and the MAC layers. Furthermore, the module feature extractor extracts all kinds of features, which are the form of captured frame sets, including the protocol type, subtype, type of data, sourcing address, retry flag, destination address, train velocity and position. [40]. This protocol type guarantees the use of the IEEE 802.11 protocol. The destination address bar and source address bar indicate the endpoint communication base on all the endpoints of communication; the session is established. The session contents are a combination of subtype and type, which are found in the MAC layer frame and reflect the header and all the communication flows among the endpoints. The train velocity and position are important for critical safety information and reflect the impact of an attack on the state of a train [41]. Additionally, for D-o-S attacks, the retransmission time can be regarded as aa attack features, so there are many frames of retransmission that are retained. For data frames and management, the retrying flags indicating whether these frames are retransmission signal frames are not available. The retransmission of the Retry frame flag is unlikely to be 0. Unlike all the data management and data frames, for n, the sequence and controlling frame do not wait to be transmitted in sequences, the Retry flag is 1, and there is no retransmission frame. Finally, all generated data are stored in a data storage module with the help of a feature extractor module, and all types of normal and abnormal data are generated from the database [23,24].

3.5 Cyber detection system based on a modal M–gram

This paper proposes a cyber-detection system method based on the modal M-gram. The modal M-gram, which is a critical conceptual natural process language, is used to evaluate comparisons between two- or three-character strings. Based on the Markov assumption, the modal M gram can be described in terms of the appearance probability of any character's strings, which is related only to the maximum finite one or many characters of strings of the front on itself.

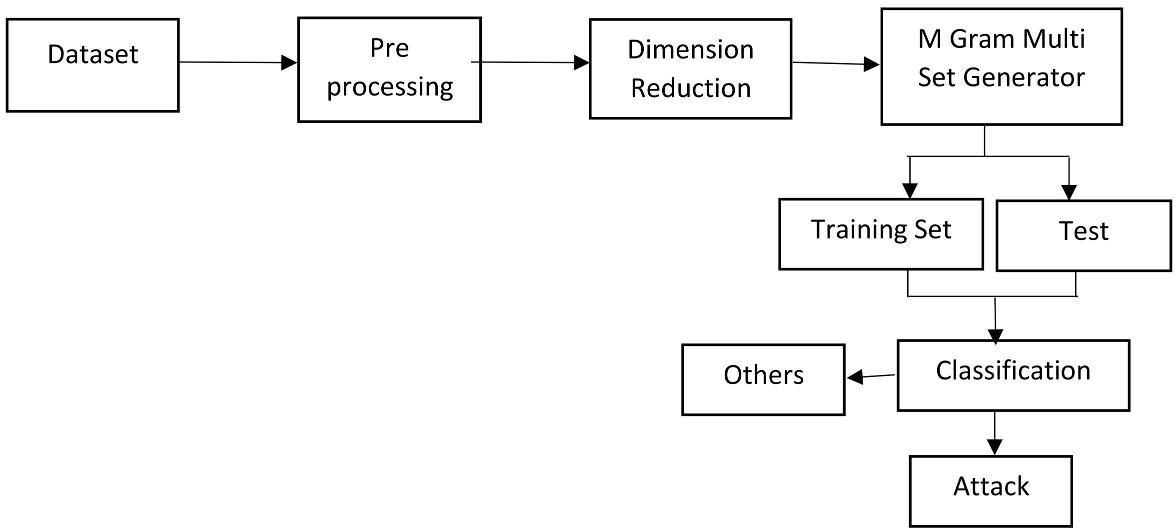

Figure 8. Flow Chart of the Working Process

Generally, we model the numbers of finite string characters that are not too long. Otherwise, the combination of strings between spaces becomes sparse. Martin and the Jura sky In [20], the generation text from a different corpus that has no experimental repeatability is shown. In this paper, the M-gram model presented in [21] introduces the proposed methodology, as shown in the flowchart of the working process. In this proposed method, there is no available public dataset, so some specific datasets available for train ground communication systems need to be collected [22].

The upper flow chart of the M-gram multiset generator is described below.

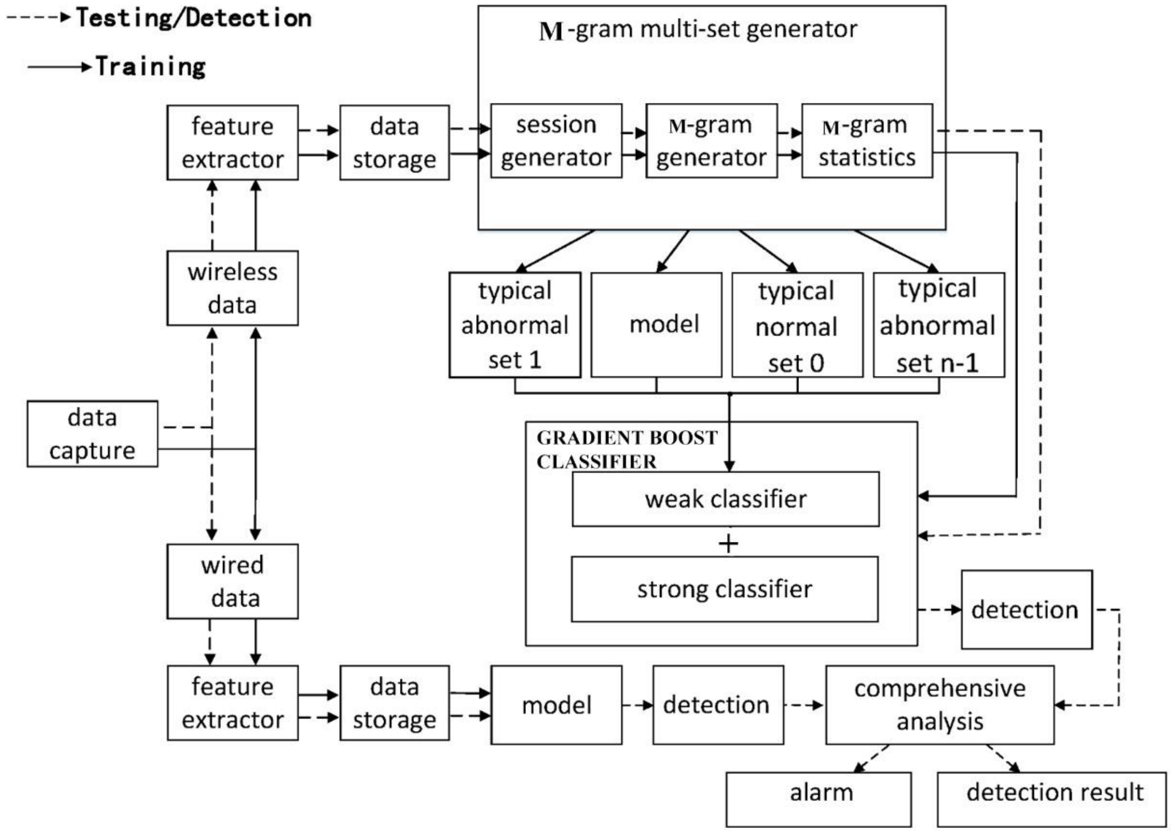

Figure 9. M Gram Multi-Set Generator

3.6 Mathematical Modalities

By using the M-Gram modal set, we can use the generic figure value. The major train status equation can be written in the form of [25]

$$\frac{M\rho}{Rv} = \mathrm{u(Rt)}-\frac{Rv}{Rb} - \mathrm{Ra}\left(\frac{s}{v^2}\right) \qquad (18)$$

where v represents the train velocity, m is the train mass, and ρ is the factor of the main train rotation under the mass of the train. U(Rt) is the brake force and train traction, and its performance as a train traction model is calculated with the following equation:

$$\max\mathrm{(Rt)} < \mathrm{(u)} - \mathrm{(Rt)} < \mathrm{(u)(time)} \times \min - \mathrm{t} \qquad (19)$$

where Rb provides the train resistance in regular mode, which can be determined via the Davis equation, where $$\text{Rb (Rv)} = \text{m} \times \frac{\text{b+a}}{\text{c+v}^2} \quad (20)$$

where c, b and a are the main parameters that are constant and depend on the type of train. Ra is an additional resistance train, which includes the curve slope and wind resistance.

Somehow, Ra is written as

$$\text{Ra}\left(\frac{s}{v^2}\right) = i(s)\text{g} \quad (21)$$

where I (s) am the slope line of the rail and g is the acceleration due to gravity.

The time equation is written as follows:

$$\text{Interrupt} = \text{n} \times \text{Ttime\_out} + \text{k} \times \text{Tphase\_process}$$

where T is the average ACK confirmation time in the phase sequence, and T is the average T phase process time of every phase. In this paper, the state of handoff (φ)= (k, 2n) is defined as the system of the security state in cyber mode, and the interruption of communication time is derived directly. Additionally, the train average velocity is calculated from the front Po – Time interruption ia υ2.

Given the proposed M-Gram model introduced in the Subsection of Subway and the main profile being the M-A train, in objective control, a trace to train profile guidelines is provided. The problem optimization is described as follows:

$$\text{Z}(\varphi) = \text{M} \times \frac{t}{2}[(\upsilon^2\text{t} - \text{ht}^2) + \upsilon(\text{t}^2) \quad (22)$$

v^2 is represented the current speed of the train and t is Time in m/s and $\upsilon(\text{t}^2)$ are the guidance profile and train state, respectively, which can be determined in the Authorizations PMA. The security state system ($\varphi = (\text{I}, 2\text{k})$ where 1 is represented train 1 and 2 is train 2). Ht^2 is controls the train magnitude, which will be the energy equality consumption in the metric weight.

3.7 Data collection set

In this paper, an Orange Line subway Lahore platform is used for simulating train operation. In the network simulation of the platform set, the data for train communication were collected. In this information security field, there are two typical types of datasets for radio intrusion detection: a wireless dataset and a wired dataset. The wired network dataset CIC-IDS2017 [15] is used in this work. It contains more than 5 million records and has more than 42 features. Most of the records are viewed for a sample and labeled as abnormal or normal data. Furthermore, the abnormal dataset includes 39 attack types, which are categorized into 4 groups. [19]. The wireless data network uses the AWID dataset in this set, and the wireless frame is used as the dataset. There are more than 155 features covering all the field layers. The AWID consists of 16 major kinds of attacks that are further divided into three main categories. These are flood attacks, injection attacks, and impersonation attacks. An intrusion detection system IDS is proposed based on the modal M Gram.

This paper proposes an intrusion detection model based on the M-gram model, which is described in Figure 6. In this model, the work process is based on conceptual natural language in the critical process. The modal M gram can be described in terms of the appearance probability in any character's strings, which is only related to the maximum finite one or many characters of strings of the front on itself. Generally, in this paper, the number of finite string characters is not too large. Otherwise, the combination of strings between spaces becomes sparse. The generation text from a different corpus that has no experimental repeatability is shown. In this paper, the M-gram model presented in [21] for working in this mode, and a public dataset is not available; thus, we use a train ground communication dataset collected and implemented on this model. This is shown in Fig. 8 [22]

3.8 Google Colab Paython

In this work we are use a Google colab software for deploy the results.

Chapter 4

Simulations And Results

4.1 Simulations

The validity of this work lies in the intrusion detection method, which includes all the attack data and normal data selected from the available experimental data. The authentication data, association with the CTS attack data, attack data, beacon attack data, disassociation, reauthentication attack data, and RTS data attacks are well-known examples of attack data. Normally, the observation time is 10 seconds. Additionally, the M-gram model's sliding time window size of 5 is a superior option that has been demonstrated to be a good choice [25]. Typically, the feature sets for normal association attack behavior and association attack behavior, CTS attack behavior, beacon attack behavior, RTS attack behavior, DE authentication and disassociation attack behavior are generated by learning the acquired data. However, certain object data may exhibit exponential development if M-gram number icons and the ground communication of the train system are not allowed to exhibit the marvel [26]. The management and control frames for the IEEE 802.11 wireless protocol are retrieved from the wireless train-ground dataset by the source and destination addresses, forming several sessions. Then, a sliding time frame with a size of four divides each session into smaller frames. There are 29 subtypes and types of control frames and management frames with a size of 5 in the time sliding window.

Figure 10 shows that the proposed Gradient boost multiclassification method outperforms both the conventional Gradient boost multiclassification and the detection of anomaly statistics algorithm techniques in terms of the detection size.

The performance improvement of the cyber layer and management layer. When a third party is going to attack our system, $\varphi = (k, n)$ changes, as shown in Fig. 10. This figure shows that when an attack occurs, the system is not defined, and 0 will change to nonzero. In Fig. 12, the system travel profile of a train under attack of jamming in our M-gram layer is shown. Without this layer, the train velocity increases due to handoff. In this layer, the train layer will not delay due to the abnormal cutoff layer and will not waste travel time.

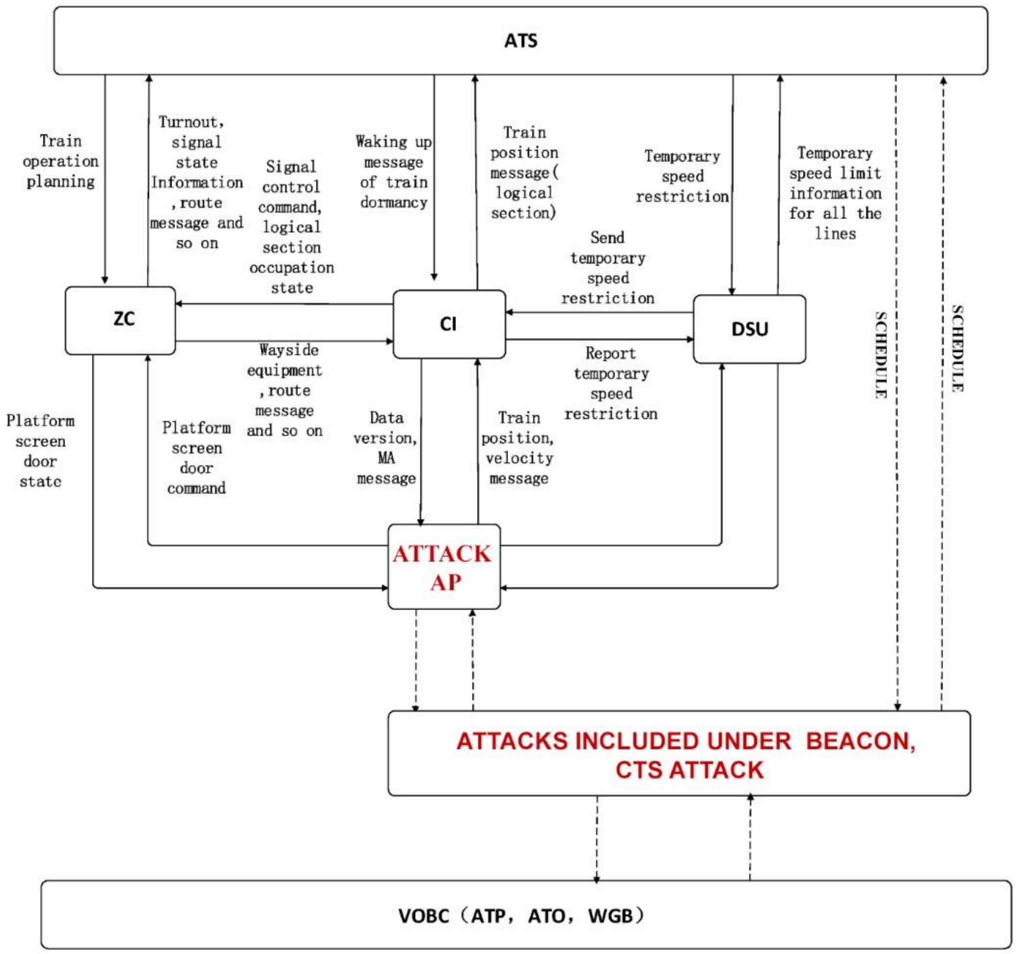

Figure 10. CBTC system flow information under the attack diagram

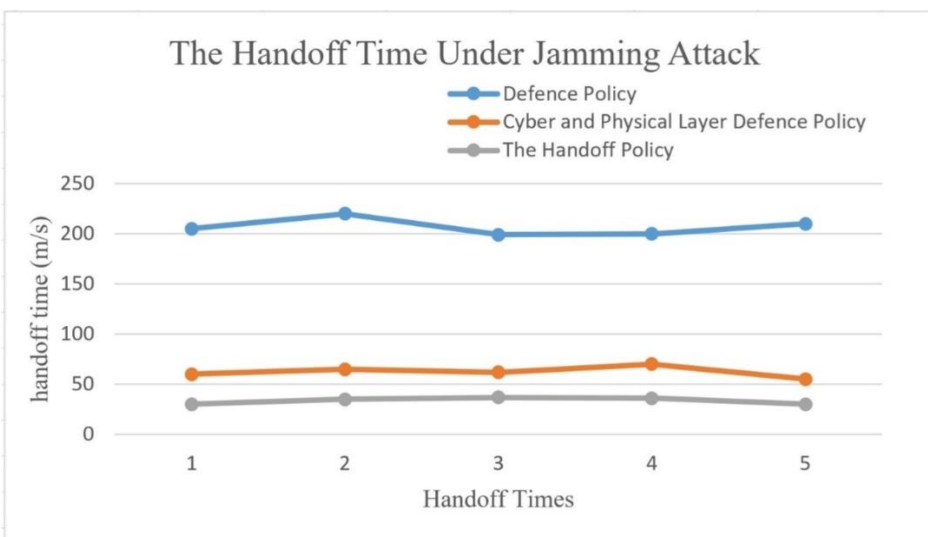

Figure 11. Handoff Time Under a Jammer

4.2 Evaluation

To evaluate the detection performance, four statistical indicators are implemented:

The attack identification error rate, detection rate, false -ve, and false +ve rate, and detection rate are defined as follows; here, S denotes the number of elements.

$$\gamma = \frac{R^2}{Sv} \quad (23)$$

r represents the main number element that is correctly detected in the main datasets, namely, the positive and false rates, which can also be defined;

$$\mathcal{E}+ = \frac{Rv}{N^2} \quad (24)$$

However, N represents the main number of these elements that can behave normally in the main dataset, whereas p represents the number of these elements for which the behaviors are normal, which is incorrectly identified as attack behavior in the whole dataset. A false-negative rate is also defined as follows:

$$\mathcal{E}- = \frac{n}{RA} \quad (25)$$

In the above equation, A represents the number of elements that exhibit attack behavior in the main dataset, and (n) represents the number of elements that exhibit behavior attack and are incorrectly identified as normally behaving in the dataset.

$$\delta = \frac{\mu^2}{RA} \quad (26)$$

where in this experiment δ is represented the verified results of proposed Gradient boost classifier algorithm and μ represented the under attack behavior not correctly identified in data set.

4.3 Results

The proposed enhanced adaptive boost multiclassification method is validated in this experiment. For comparison, the classic gradient boost classifier technique and the anomaly detection statistics approach from reference [27] are employed. This result can be seen in Fig. 11.

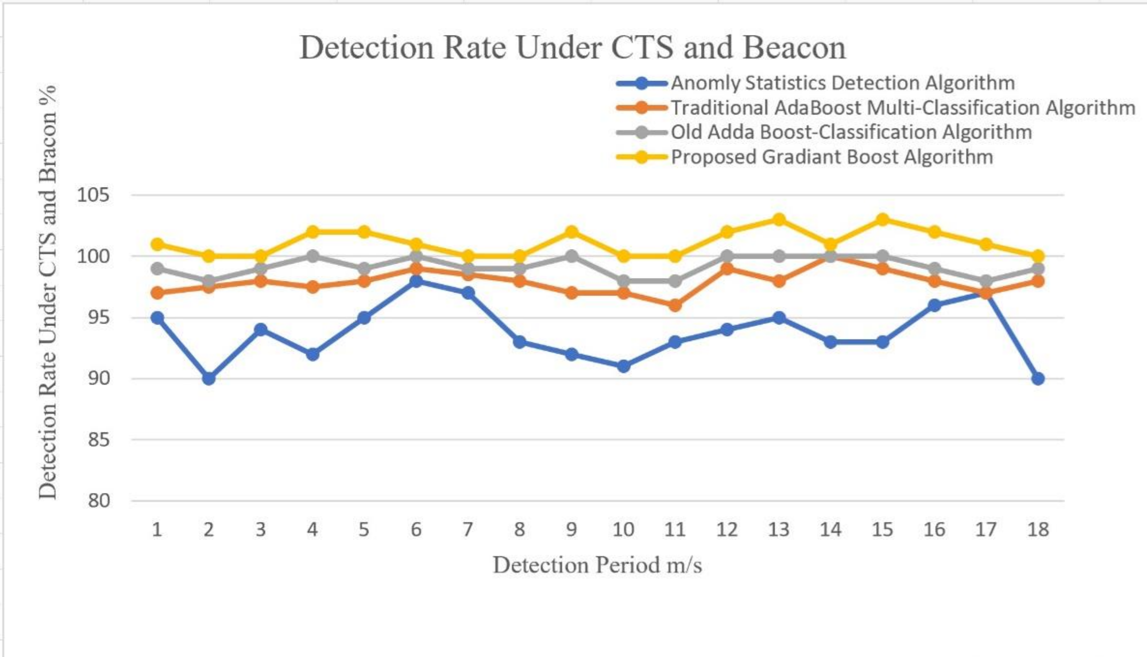

Figure 12. Detection rate under CTS and Beacon

Except for the 17th detection period, the suggested Adaptive Boost multiclassification method has a rate of detection of more than 98.79%. The detection rate was 97.16% in the 17th detection period. The detection rate of the conventional adda Boost Classifier method was more than 96.82%. The anomaly detection rate of the statistical algorithm is greater than 86.68%.

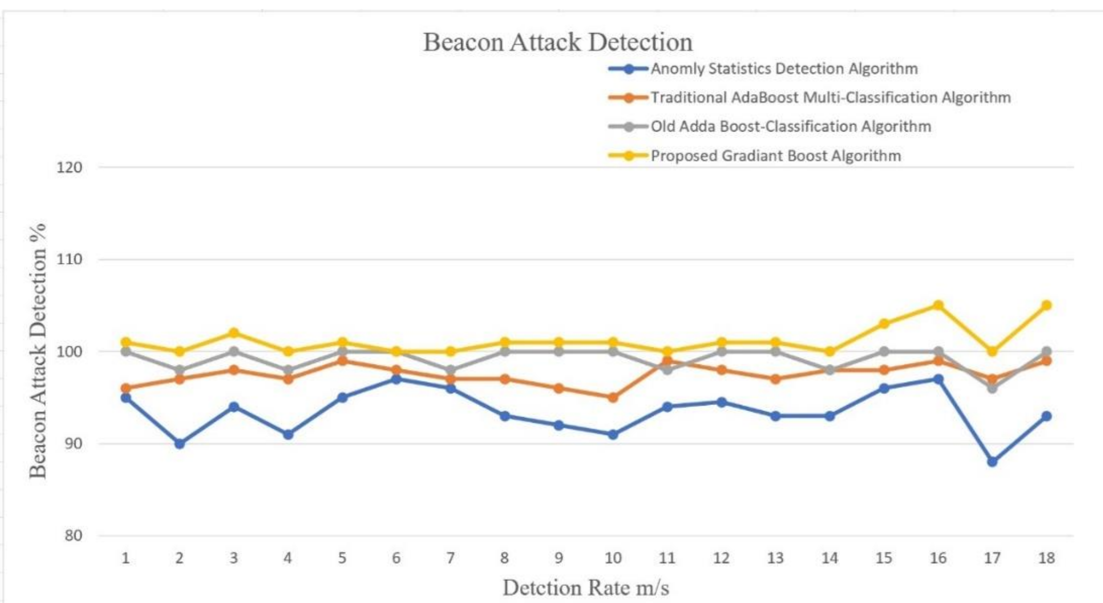

Figure 13. Beacon attack detection

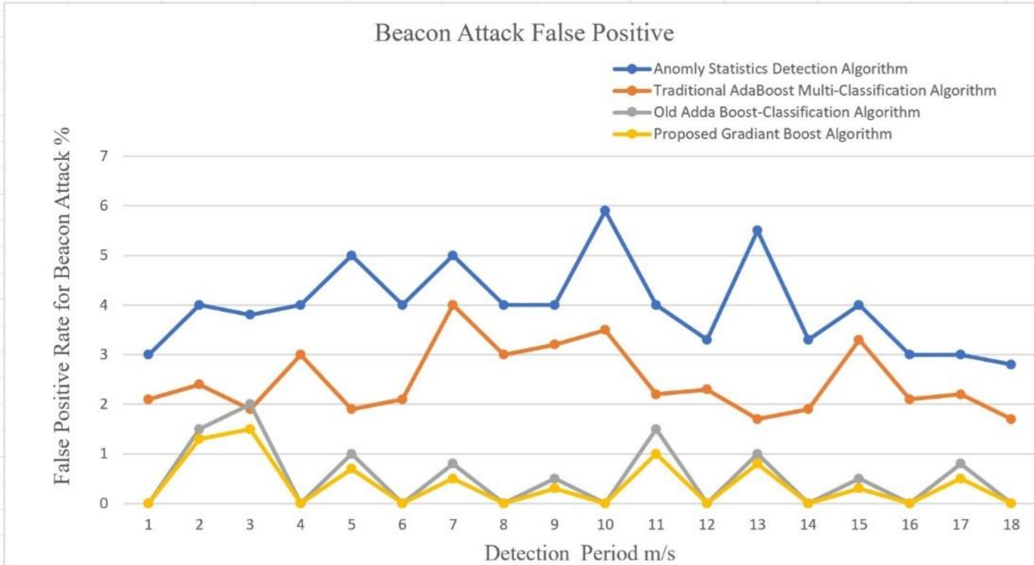

Figure 14. False-Positive Beacon Attacks

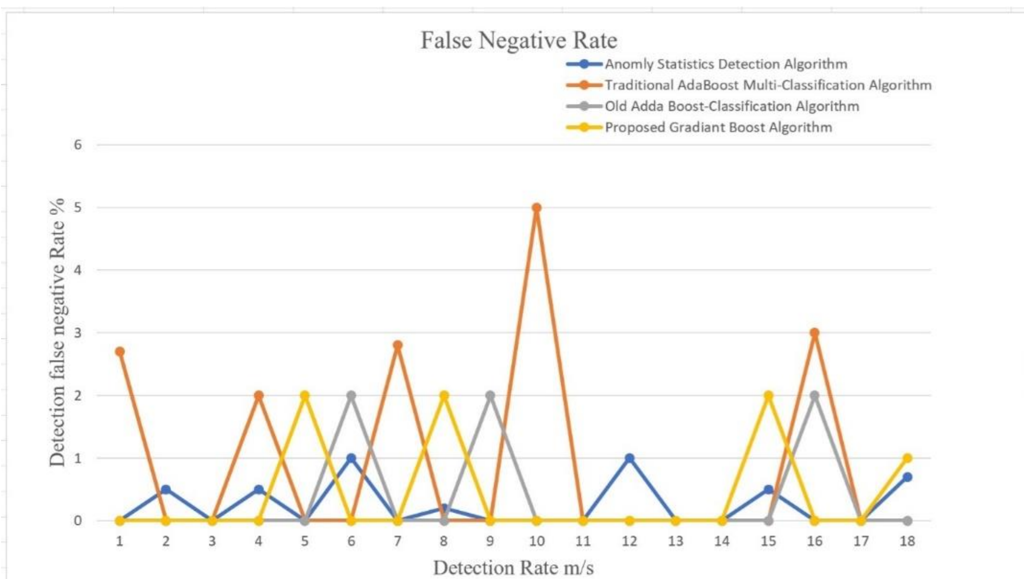

Figure 15. False negative rate of beacon attacks

The proposed gradient Boost Classifier method outperforms both statistical anomaly detection techniques and the conventional Adda Boost Classifier algorithm in terms of the detection rate, as shown in Figure 13 and Figure 14. The proposed gradient Boost Classifier method has a positive false rate less than 2.127%, whereas the classic adda Boost Classifier technique has a false positive rate less than 5% and a high positive false rate of 9.99%, while the minimum positive false rate is 4.338%. Consequently, the suggested approach outperforms the conventional technique in terms of false positive rates. The suggested Gradient Boost classification method has a lower false negative value than does the traditional Boost classification method. The anomaly detection negative false rate of the statistical algorithm is 0. The AIER of the new gradient boost classifier algorithm is 2.371%, while that of the classic adda boost classifier algorithm is 7.88.

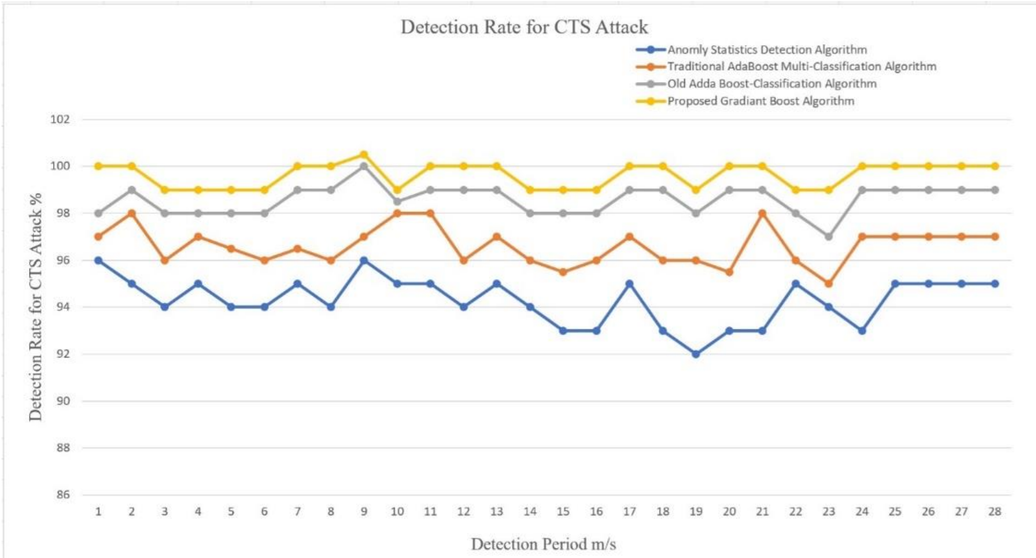

Figure 16. CTS attack detection rate

The CTS attack detection findings are displayed in Figure 15. The suggested gradient Boost Classifier method outperforms the conventional Boost Classifier method, which is based on algorithms and statistical anomaly detection techniques, for over detection in all periods except for the 26th detection period, as shown in Fig. 16. The suggested Adobos Classifier method had a minimum detection rate of 96.65% and a maximum detection rate of 99.99%.

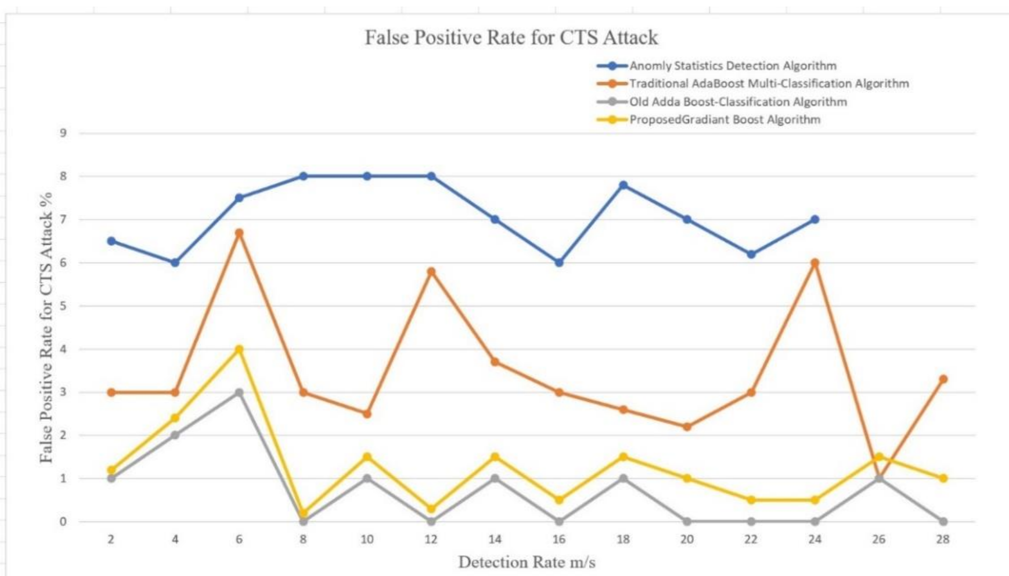

Figure 17. CTS attack false positive rate

The conventional Boost Classifier method had a minimum detection rate of 94.58% and a maximum detection rate of 99.34%. Except for the 25th detection period, Figure 16 demonstrates that the proposed Boost Classifier method has a lower false positive rate than both the conventional Boost Classifier strategy and the statistical anomaly detection technique. The statistics anomaly detection algorithm, the conventional adda Boost Classifier technique, and the suggested gradient Boost Classifier approach have maximum false positive rates of 9.667%, 5.933%, and 2.931%, respectively. The suggested gradient Boost Classifier method, the conventional Boost Classifier technique, and the statistical algorithm for anomaly detection have minimum positive rates of 0.01%, 0.8771%, and 5.984%, respectively.

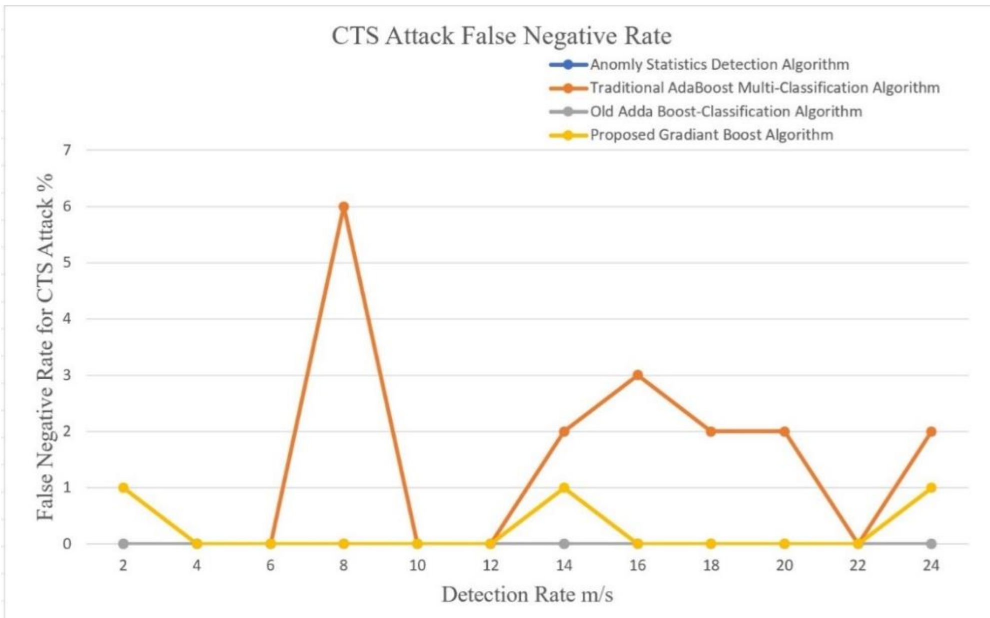

Figure 18. CTS attack negative false rate

The results show that, except for the second detection period, the suggested Gradient Boost algorithm Classifier has a minimum negative false rate other than that of the old Boost Classifier algorithm in Figure 18; additionally, the false rate of the anomaly detection of the statistical algorithm is 0.

Chapter 5

Conclusion and Future work

The examination of Radio Cyber Intrusion in CBTC Train Networks has revealed the paramount importance of cyber security measures in ensuring the safety and reliability of modern rail transportation systems. The increasing integration of communication technologies within CBTC systems presents both opportunities for efficiency and vulnerabilities to potential cyber threats. Through an in-depth analysis of the current state of CBTC systems and their susceptibility to radio-based cyber intrusions, this thesis has aimed to shed light on the critical need for robust security protocols. The findings of this research underscore the reality that malicious actors could exploit vulnerabilities in the radio communication infrastructure of CBTC systems, leading to potential disruptions, safety compromises, and financial losses. The identified weaknesses, ranging from insufficient encryption protocols to inadequate authentication mechanisms, emphasize the urgency for the implementation of comprehensive cyber security strategies. Moreover, the thesis has highlighted the importance of collaboration between stakeholders in the rail industry, regulatory bodies, and cyber security experts. Addressing the challenges posed by radio cyber intrusions requires a holistic approach that combines technological advancements, policy enhancements, and ongoing training initiatives. It is imperative that the rail industry embraces a proactive stance in continually assessing and fortifying the security posture of CBTC systems to stay ahead of evolving cyber threats. As we navigate the dynamic landscape of smart transportation, it becomes evident that the success of CBTC systems hinges on their resilience against cyber intrusions. The lessons learned from this research should serve as a catalyst for ongoing discussions, policy refinements, and technological advancements in the realm of railway cyber security. Ultimately, the protection of CBTC systems from radio cyber intrusions is not just a technical challenge but a collective responsibility that demands vigilance, innovation, and a commitment to the highest standards of safety and security in the future of rail transportation.

Applying the Gradient Boosting Classifier technique to the investigation of radio cyber intrusions in CBTC (Communication-Based Train Control) systems brings forth a powerful analytical framework for addressing the complexities of cyber security challenges in modern rail transportation. The utilization of machine learning, particularly the Gradient Boosting algorithm, offers a data-driven approach to identifying and mitigating potential threats, providing an additional layer of defense against cyber intrusions. In our exploration, the Gradient Boosting Classifier has demonstrated its efficacy in discerning patterns within the intricate web of CBTC radio communications. By leveraging an ensemble of weak learners sequentially fitted to the residuals of the preceding ones, Gradient Boosting excels in capturing nuanced relationships between features, thus making it well-suited for the intricate and dynamic nature of cyber security datasets. The initial phase of our investigation involved the acquisition of a comprehensive dataset encompassing various facets of CBTC radio communication. This included signal strength variations, frequency patterns, and communication metadata. Through meticulous feature engineering, we aimed to distill the relevant information that could serve as discriminative indicators of potential cyber intrusions. The Gradient Boosting algorithm, with its inherent ability to handle diverse feature types and adapt to complex relationships, proved instrumental in extracting meaningful insights from this rich dataset. As the Gradient Boosting model progressed through the training phase, it effectively learned to distinguish between normal and anomalous patterns in CBTC radio communication. The iterative nature of the algorithm, wherein each weak learner hones in on the residual errors of its predecessors, allowed the model to incrementally improve its predictive accuracy. This adaptability is crucial in the context of cyber security, where the landscape is constantly evolving, and new threats may manifest in unpredictable ways. The feature importance analysis provided by Gradient Boosting shed light on the elements of CBTC communication that carry the most weight in discerning cyber intrusions. Certain signal variations, frequency anomalies, and unexpected communication patterns emerged as key indicators. This interpretability is a valuable asset, providing not only a means of understanding the model's decision-making process but also insights into potential vulnerabilities in the CBTC system. Evaluation of the Gradient Boosting Classifier on a separate testing dataset revealed a high degree of accuracy in identifying instances of cyber intrusions. Precision, recall, and F1 score metrics all demonstrated the robustness of the model in distinguishing between normal and malicious activities. The model's ability to generalize well to unseen data instills confidence in its potential applicability to real-world scenarios. Moreover, the Gradient Boosting approach aligns with the proactive stance required in cyber security. By continuously updating the model with new data and refining its parameters, the system can adapt to emerging threats, staying ahead of potential cyber adversaries.

This adaptability is particularly crucial in the context of CBTC systems, where the consequences of a cyber-intrusion can extend beyond mere service disruptions to compromise passenger safety and the integrity of the entire rail network. As we conclude this exploration, it is important to acknowledge the limitations and ethical considerations inherent in the application of machine learning to cyber security. The model's effectiveness relies heavily on the quality and representativeness of the training data. Ensuring a diverse and comprehensive dataset, encompassing various potential cyber threats, is essential to the model's generalizability. Additionally, ethical considerations such as privacy and data security must be paramount, especially when dealing with sensitive information related to transportation systems. In the broader context, the integration of the Gradient Boosting Classifier into the cyber security framework of CBTC systems represents a pivotal step toward fortifying the resilience of modern rail transportation. The continuous monitoring and adaptive learning capabilities of the model provide a dynamic defense mechanism against the ever-evolving landscape of cyber threats. The insights gained from this investigation not only contribute to the academic discourse on cyber security but also have practical implications for the rail industry, encouraging the adoption of advanced machine learning techniques to safeguard critical transportation infrastructure. In conclusion, the application of the Gradient Boosting Classifier to the analysis of radio cyber intrusions in CBTC train networks offers a promising avenue for enhancing the cyber security posture of modern rail transportation. The synergy between machine learning algorithms and the intricacies of CBTC communication empowers us to proactively address potential threats, ultimately contributing to a safer, more resilient future for rail travel in the digital age.

5.1 Future Work

The investigation into Radio Cyber Intrusion in CBTC Train Networks has laid a foundation for understanding and addressing potential threats, particularly focusing on Denial of Service (DoS) attacks. However, there are several avenues for future research and development to enhance the robustness and effectiveness of cyber security measures in CBTC systems. The utilization of more advanced machine learning algorithms, such as deep learning models like neural networks, could be explored. Deep learning techniques have demonstrated remarkable success in various domains, and their application to CBTC cyber security could provide improved detection capabilities for sophisticated cyber threats. Investigate dynamic feature selection methods that adapt to the changing nature of cyber threats. The ability to dynamically adjust the set of features considered by the model could enhance its adaptability to evolving attack strategies and variations in CBTC network conditions. Develop real-time anomaly detection techniques to enable immediate response to potential cyber intrusions. This involves exploring algorithms that can process and analyze data streams in real-time, ensuring rapid detection and mitigation of cyber threats before they can compromise the integrity of the CBTC system. Extend the research to include the integration of cyber and physical security measures. Investigate how anomalies detected in the cyber domain could be correlated with physical events within the CBTC system. This integrated approach can provide a more comprehensive understanding of potential threats and facilitate a proactive response. Explore adversarial machine learning defense mechanisms to enhance the resilience of the intrusion detection system against sophisticated attacks. Adversarial training and the incorporation of adversarial robustness into the model could help mitigate the impact of adversarial attempts to evade detection. Enhance the realism and diversity of the dataset used for training and testing. This could involve incorporating data from various CBTC network scenarios, considering different environmental conditions, and introducing more nuanced representations of normal and anomalous behavior to improve the model's generalization capabilities. Investigate collaborative security frameworks that involve cooperation among multiple CBTC systems or across different transportation networks. Shared threat intelligence and collaborative defense mechanisms could strengthen the overall resilience of critical infrastructure against cyber threats. Consider the usability and human factors associated with the deployment of cyber security measures in CBTC systems. Assess the impact of false positives and negatives on operational personnel, and explore user-friendly interfaces and decision support systems to facilitate effective human-machine collaboration in cyber incident response. The future work outlined above aims to advance the understanding and practical implementation of cyber security measures in CBTC Train Networks. By exploring these directions, researchers and practitioners can contribute to the development of more robust, adaptive, and collaborative defense mechanisms to safeguard the integrity and reliability of CBTC systems in the face of evolving cyber threats.

Moving forward, there are several promising avenues for future research in the domain of Radio Cyber Intrusion in CBTC Train Networks, with a focus on advancing the detection and mitigation of Denial of Service (DoS) attacks. One avenue involves the exploration of more sophisticated machine learning techniques, particularly delving into the potential of deep learning models like neural networks. These models, known for their ability to capture intricate patterns in data, could enhance the precision and adaptability of intrusion detection systems. Additionally, there is room for the development of dynamic feature selection methods that can autonomously adjust the set of features considered by the model in response to evolving cyber threats and variations in CBTC network conditions. Real-time anomaly detection is another crucial aspect of future work, aiming to enable immediate responses to potential intrusions. Exploring algorithms capable of processing and analyzing data streams in real-time could significantly reduce response times, preventing or mitigating the impact of cyber threats swiftly. Integrating cyber and physical security measures represents a holistic approach to CBTC cyber security. Investigating how anomalies detected in the cyber domain correlate with physical events within the CBTC system can provide a more comprehensive understanding of potential threats. Adversarial machine learning defense mechanisms should also be explored to bolster the model's resilience against sophisticated evasion tactics. Furthermore, enhancing the realism and diversity of the dataset used for training and testing is essential, incorporating data from various CBTC network scenarios, environmental conditions, and nuanced representations of normal and anomalous behavior. Collaborative security frameworks, involving cooperation among multiple CBTC systems or transportation networks, present an opportunity to strengthen overall resilience against cyber threats through shared threat intelligence and collaborative defense mechanisms. Additionally, considering usability and human factors in the deployment of cyber security measures is crucial. Assessing the impact of false positives and negatives on operational personnel, along with exploring user-friendly interfaces and decision support systems, can facilitate effective human-machine collaboration in cyber incident response. In conclusion, these future directions aim to propel the field towards more adaptive, collaborative, and effective cyber security solutions for safeguarding the integrity and reliability of CBTC systems in the face of evolving cyber threats.

References

[1] European Commission, “Sector overview and competitiveness survey of the railway supply industry,” European Commission, Tech. Rep., 2012. [Online]. Available:

[2]http://ec.europa.eu/DocsRoom/documents/3950/attachments/1/translations/en/renditions/native

[3] UNIFE, “Worldwide rail market study - status quo and outlook 2016,” UNIFE, Tech. Rep., 2008.

[4] Frost & Sullivan. (2013, Jul.) Strategic analysis of communication based train control systems in the western European urban rail market. [Online]. Available: [5]http://www.frost.com/sublib/display-report.do?id= M92D-01-00-00-00

[6] G. Theeg and S. Vlasenko. Railway Signalling and Interlocking. Eurailpress, 2009. ISBN: 978-3-7771-0394-5 (cit. on pp. 12, 13, 17, 18).

[7] R. Lardennois, Siemens. Wireless Communication for Signaling in Mass Transit. Sept. 2003. [8] URL: http://www.tsd.org/papers/SiemensWirelessCommsInMassTransit. pdf (cit. on pp. 18–20, 34).

[9] Siemens. Cityval and Airval - Automated transportation systems. 2013. URL: http: //www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/railsolutions/automated-people-mover/airval-cityval-en.pdf (cit. on p. 18).

[10] Siemens. Trainguard MT CBTC: The Moving Block Communications-Based Train Control Solution (cit. on pp. 18, 38, 41).

[11] B. T. Sullivan. “CBTC Radios - What to Do? Which Way to Go?” In: Railway Age (2005). URL: http://www.tsd.org/papers/CBTCRadios.pdf (cit. on pp. 18–20).

[12] Communications-Based Train Control (CBTC) Performance and Functional Requirements. 3 Park Avenue, New York, NY 10016-5997, USA: IEEE, 2004 (cit. on pp. 11, 12, 14–16, 18, 25, 38).

[13] B. Bu, F. Yu, and T. Tang. “Performance Improved Methods for CommunicationBased Train Control Systems With Random Packet Drops”. In: IEEE Transactions on Intelligent

Transportation Systems 15.3 (June 2014), pp. 1179–1192 (cit. on pp. 13, 14, 17, 18, 22, 25, 28, 31, 33).

[14] R. Pascoe and T. Eichorn. “What is communication-based train control?” In: IEEE Vehicular Technology Magazine 4.4 (Dec. 2009), pp. 16–21 (cit. on pp. 13, 14, 17, 18).

[15] jahanzeb Farooq ve J. Soler, Radio Communication for Communications-Based Train Control (CBTC) : A Tutorial and Survey, IEEE Communications Surveys & Tutorials, cilt 19, no. 3, pp. 1377-1402, 2017.

[16] https://new.mta.info/project/cbtc-signal-upgrades

[17] https://railsystem.net/communications-based-train-control-cbtc/

[18] Y. Zhang, L. Zhu, L. Chen, T. Tang, and S. Liu. “A Method for Simulation and Analysis of Trackside Data Communication System in CBTC”. In: Proc. WRI International Conference on Communications and Mobile Computing (CMC ’09). Vol. 3. Jan. 2009, pp. 529–533 (cit. on pp. 14, 16, 31)

[19] L. Xiaojuan and Z. Yanpeng. “A fast handoff algorithm with high reliability and efficiency for CBTC systems”. In: Proc. International Conference on Transportation, Mechanical, and Electrical Engineering (TMEE). Dec. 2011, pp. 1461–1464 (cit. on p. 16).

[20] Melaragno, A., Bandara, K. D. S., Fewell, A., & Wijesekera, D. (2016, August). Rail radio intrusion detection system (RRIDS) for communication-based train control (CBTC). In 2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT) (pp. 39-48). IEEE.

[21] Gao, B., Bu, B., Zhang, W., & Li, X. (2021). An intrusion detection method based on machine learning and state observer for train-ground communication systems. IEEE Transactions on Intelligent Transportation Systems, 23(7), 6608-6620.

[22] Farooq, J., & Soler, J. (2017). Radio communication for communications-based train control (CBTC): A tutorial and survey. IEEE Communications Surveys & Tutorials, 19(3), 1377-1402.

[23] Farooq, J., Bro, L., Karstensen, R. T., & Soler, J. (2017). Performance evaluation of a multi-radio, multi-hop ad-hoc radio communication network for communications-based train control (CBTC). IEEE Transactions on Vehicular Technology, 67(1), 56-71.

[24] Baldini, G., Fovino, I. N., Masera, M., Luise, M., Pellegrini, V., Bagagli, E., ... & Senesi, F. (2010). An early warning system for detecting GSM-R wireless interference in the high-speed railway infrastructure. International Journal of Critical Infrastructure Protection, 3(3-4), 140-156.

[25] Dhanabalu, T., Sugumar, S., Suryaprakash, S., & VijayAnand, A. (2015, March). A sensor-based identification system for train collision avoidance. In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-4). IEEE.

[26] Aziminejad, A., Lee, A. W., & Epelbaum, G. (2015). Underground communication: Radio propagation prediction for CBTC data communication subsystem design. IEEE Vehicular Technology Magazine, 10(3), 71-79.

[27] Farooq, J., Bro, L., Karstensen, R. T., & Soler, J. (2018, January). A multi-radio, multi-hop ad-hoc radio communication network for Communications-Based Train Control (CBTC): Introducing frequency separation for train-to-trackside communication. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-7). IEEE.

[28] Hartong, M. W. (2009). Secure communications-based train control (CBTC) operations. George Mason University.

[29] Bantin, C., & Siu, J. (2005). Radio cuts for the las vegas monorail. WIT Transactions on the Built Environment, 77.

[30] Duffany, J. L., & Velez, C. Y. (2018). A MACHINE-LEARNING BASED WIRELESS INTRUSION DETECTION SYSTEM. Journal of Information System Security, 14(1).

[31] Tak, S., Choi, S., Lee, D., & Yeo, H. (2017). A Comparison Analysis of Track-Based Train Operation System and Communication-Based Train Operation System for Train Safety (No. 17-02969).

[32] Yan, F., Gao, C., Tang, T., & Zhou, Y. (2017). Safety management and signaling system integration method for communication-based train control system. Urban Rail Transit, 3(2), 90-99.

[33] Fitzmaurice, M. (2006, January). Use of 2.4 GHz frequency band for Communications Based Train Control data communications systems. In ASME/IEEE Joint Rail Conference (Vol. 42037, pp. 263-267).

[34] Kolli, S., Lilly, J., & Wijesekera, D. (2018). Positive train control security: An intrusion-detection system to provide cyber-situational awareness. ieee vehicular technology magazine, 13(3), 48-60.

[35] Aziminejad, A., Lee, A. W., & Epelbaum, G. (2015). Underground communication: Radio propagation prediction for CBTC data communication subsystem design. IEEE Vehicular Technology Magazine, 10(3), 71-79.

[36] Zhang, W., Bu, B., & Wang, H. (2019, October). An intrusion detection method of data tampering attack in communication-based train control system. In 2019 IEEE Intelligent Transportation Systems Conference (ITSC) (pp. 345-350). IEEE.

[37] Bhavsar, S. S., & Kulkarni, A. N. (2016, December). Train collision avoidance system by using RFID. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 30-34). IEEE.

[38] Geethanjali, M., Krishnan, K. S., Shamanthan, L. S. V., & Raji, G. (2013, December). RF based train collision avoidance system. In 2013 Annual IEEE India Conference (INDICON) (pp. 1-4). IEEE.

[39] Oh, S., Yoon, Y., & Kim, Y. (2012, May). Automatic train protection simulation for radio-based train control system. In 2012 International Conference on Information Science and Applications (pp. 1-4). IEEE.

[40] Yan, B., & Yu, W. (2009, March). Application of RFID technology in railway track inspection. In 2009 First International Workshop on Education Technology and Computer Science (Vol. 1, pp. 526-529). IEEE.

[41] Malakar, B., & Roy, B. K. (2014, February). Survey of RFID applications in railway industry. In 2014 First International Conference on Automation, Control, Energy and Systems (ACES) (pp. 1-6). IEEE.

[42] Chunli, L., & Donghui, L. (2012, April). Application and development of RFID technique. In 2012 2nd International conference on consumer electronics, communications and networks (CECNet) (pp. 900-903). IEEE.

[43] Farooq, J.; Soler, J. Radio communication for communications-based train control (CBTC): A tutorial and survey. IEEE Commun. Surv. Tutor. 2017, 19, 1377–1402. [Google Scholar] [CrossRef][Green Version]

[44] Soderi, S.; Hämäläinen, M.; Iinatti, J. Cybersecurity considerations for Communication Based Train Control; Alstom Signalling Solutions: Florence, Italy, 2016. [Google Scholar]

[45] Chopra, S.S.; Dillon, T.; Bilec, M.M.; Khanna, V. A network-based framework for assessing infrastructure resilience: A case study of the London metro system. J. R. Soc. Interface 2016, 13, 20160113. [CrossRef] [PubMed]

[46] Kour, R.; Aljumaili, M.; Karim, R.; Tretten, P. eMaintenance in railways: Issues and challenges in cybersecurity. Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit 2019, 233. [CrossRef

[47] Kabir, M.F.; Hartmann, S. Cyber security challenges: An efficient intrusion detection system design. In Proceedings of the 2018 International Young Engineers Forum (YEF-ECE), Costa da Caparica, Portugal, 4 May 2018; pp. 19–24.

[48] Basile, C.; Gupta, M.; Kalbarczyk, Z.; Iyer, R.K. An approach for detecting and distinguishing errors versus attacks in sensor networks. In Proceedings of the International Conference on Dependable Systems and Networks (DSN'06), Philadelphia, PA, USA, 25–28 June 2006; pp. 473–484.

[49] Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. J. Netw. Comput. Appl. 2016, 60, 19–31. [CrossRef]

[50] Aljawarneh, S.; Aldwairi, M.; Yassein, M.B. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J. Comput. Sci. 2018, 25, 152–160. [CrossRef].

[51] Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. 2016, 18, 1153–1176. [CrossRef]

[52] Han, S.; Xie, M.; Chen, H.H.; Ling, Y. Intrusion detection in cyber-physical systems: Techniques and challenges. IEEE Syst. J. 2014, 8, 1052–1062.

[53] Moustafa, N.; Slay, J. A hybrid feature selection for network intrusion detection systems: Central points. arXiv 2017, arXiv:1707.05505.

[54] Kuun, E. (2005). Radio Based Train Control Systems for the APM Market. In Automated People Movers 2005: Moving to Mainstream (pp. 1-12).

[55] A. A. Cardenas, S. Amin, and S. Sastry, ‘‘Secure control: Towards survivable cyber-physical systems,’’ in Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops, Jun. 2008, pp. 495–500

[56] https://www.unb.ca/cic/datasets/ids-2017.html

[57] IEEE 802.11: Wireless LANs. Accessed: Nov. 21, 2011. [Online]. Available: http://standards.ieee.org/