Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# IMPROVING SECURITY IN WIRELESS MOBILE COMMUNICATION THROUGH MACHINE LEARNING: INSIGHTS FROM GSM AND TDMA APPROACHES

**RAKESH KUMAR[1], ANANT KUMAR SINHA[2], RAKESH KUMAR YADAV[3], SANTOSH KUMAR SHUKLA[4]**

[1]Research Scholar, Department of Computer science and I.T., Magadh University, Bodh Gaya, Bihar, India
[2]Associate Professor & Head, Dept. of Physics, A. M. College, Gaya. Bihar, India
[3]Associate Professor, Maharishi School of Engineering & Technology Maharishi University of Information Technology, Lucknow, India
[4] Professor, Babu Banarasi Das Institute of Technology and Management, Lucknow, India

Email: [1]rakeshmtech23@gmail.com,[2]aks26962@gmail.com, [3]rkymuit@gmail.com, [4]santosh.knmiet@gmail.com

**ABSTRACT**

Wireless communication allows for the exchange of information between numerous locations without the use of physical means like cables or optical fibers. Wireless security, a critical component of Wi-Fi networks, protects against unauthorized access and data breaches. Wireless solutions, unlike conventional communication, do not require infrastructure or cable maintenance. The research seeks to improve the user experience in wireless mobile communication by utilizing machine learning technologies for security considerations. It looks at how machine learning, together with Global System for Mobile Communication (GSM) and Time Division Multiple Access (TDMA) technologies, can be used to improve wireless security. The study predicts that as technology advances, there will be a greater reliance on wireless communication around the world. Furthermore, it underscores the importance of providing future-proof security solutions for wireless users, particularly in contexts where wiring individual devices is impractical due to the scale of digital networks.

***Keywords:*** *Machine, Machine Learning (ML), Network, Security, Technology.*

## 1. INTRODUCTION

Many industries, including the military, business, retail, manufacturing, healthcare, and transportation, have found considerable acceptance for wireless networks. These systems are utilized in networks with fixed, mobile, and ad-hoc architectures, among others. A Wireless Communication Network (WCN) is made up of thousands of tiny devices, each with the ability to sense, process, and communicate information about the outside world. These are anticipated to be crucial in a wide range of applications, from crucial military surveillance to monitoring building security and forest fires [1]. The majority of WCN deployments use unregulated International Safety Management bands (2.4GHz). The same frequency is also used by other short-range wireless protocols including Wi-Fi and Bluetooth. Because of the growing number of WCN-based apps being deployed, this band has become overcrowded [2], [3].

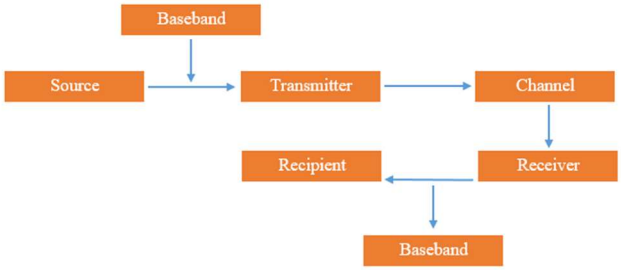


*Figure 1: Illustrating The Components Of A Wireless Mobile Communication System [4].*

The information that needs to be communicated has an origin or source. Voice, text, pictures, packet data, and other types of information can be included. On a carrier or medium known as the Baseband signal, this message is often encoded. The data to be communicated is applied to the baseband signal before transmission because the baseband signal itself is not informational. The message is subsequently transmitted by the transmitter into the

transmission medium. The channel serves as a conduit for transmitting the output of the transmitters to the receiver. A wire, coaxial cable, or optical fiber could be this in a wired system. Usually, radio or infrared waves are used in wireless systems. The receiver would be located on the opposite side of the channel. By subtraction of the baseband signal from the obtained incoming signal, it would retrieve the data from it. Data from the source is output by the receiver and can be communicated to the recipient as shown in Figure 1 [4].

The requirements of people and the advancement of wireless communication technologies go hand in hand. The future 5G (5th generation) technologies will offer a greater transmission rate, a shorter transmission latency, and more customer satisfaction than the current 4G technology. The foundation of the information society as well as the main component of the Internet of Things is machine-to-machine communication (M2M) technology [5], [6]. This article is focused on M2M technology as a result. Sensors and other technologies are used in M2M to give wireless communication equipment the ability to communicate on its own. The primary advantage of this technology is that it operates without the involvement of humans. It can thus be used in a wide range of situations, including bright transference systems, smart watching systems, electronic meters, medicinal systems, and public safety monitoring [7], [8].

Technology for 5G is continually developing. People's lives now cannot function without a wireless connection. More and more applications and services for communication are moving toward becoming wireless and portable. The vulnerability of wireless communication to network security is likewise getting more and more serious. The most noticeable aspect of wireless communication is connecting the two parties using electromagnetic waves that are traveling through the air. This offers communication users convenience and independence. Electromagnetic waves, on the other hand, can spread in all ways and are permeable [9], [10]. It can be quickly stopped as it spreads. This increases the number of potential dangers to wireless communication. Wireless communication networks have distinct insecurity concerns in wireless contexts and are vulnerable to security threats from wired networks as a result of their different transmission formats. The following issues with network security are the key ones: unauthorized listening, interference assaults, unauthorized access, and energy-consuming attacks [11]. Illegal eavesdropping occurs when an outsider monitors a wireless channel to gather information about transmission. In a jamming attack, additional jamming communication is added to the user communication network, which may cause communication failure or errors. Information about calls, locations, data, and signaling can be compromised or leaked as a result of wireless surveillance and jamming assaults [12], [13].

Due to its improved accessibility, wireless communication offers several benefits. However, it also makes sense given the numerous security dangers. Given that all communication occurs in the air, if a communication is not encrypted using a powerful algorithm or safety protocol, it can be easily accessed. While the physical transmission channel in wired networks can be guarded, the transmission medium in wireless networks is air [14], [15]. As a result, transferred data is accessible with ease. Wireless networks' mobility is another issue that leads to issues. Wireless networks come into being due to user mobility and signal transmission across the air. Therefore, with the advent of wireless networks, the issue of security and privacy issues becomes more crucial. An important aspect of a wireless network for communication is user anonymity. There are many levels of anonymity available, such as concealing the user's identity from specific administrative entities. Being accessible at any time and from any location raises serious privacy concerns among potential users. Mobile customers make use of the services offered by numerous service providers at various locations. Understanding the trust concerns connected with allowing mobile clients to access resources from several servers at different locations is crucial [16].

Wireless mobile communication, which uses cellular technology among other things, is undoubtedly a new technology that facilitates the Internet of Things. The network architecture of Wireless mobile communication is discussed changes that would result from the deployment of various MTCD-related transmission techniques. To properly balance performance and cost, one must also take into account the complexity and overhead of implementing the schemes. Wireless communication capable cellular network, it is anticipated that well-designed resource allocation methods can offer operators remarkable benefits at low costs. Wireless transmission has numerous options to increase production and cut costs. While it is impossible to eliminate all of the hazards connected to wireless communication, a solid level of overall security can be attained by using a methodical approach to assessment and

management. Several security vulnerabilities to wireless communication are covered in this study. The dangers can seriously disrupt wireless connectivity in some ways. One can assure secure wireless connectivity and avoid having their personal information trapped by following the safety rules.

The study focuses on enhancing wireless mobile communication security by integrating machine learning techniques with GSM and TDMA protocols. It assumes the availability of labeled datasets for training machine learning models, the continued relevance of GSM/TDMA-based architectures in certain regions, and the feasibility of deploying trained models on edge or cloud systems. However, the study is limited by the scarcity of real-time attack data, challenges associated with deploying ML models in low-power mobile environments, and the context-specific nature of the findings, which may not be directly generalizable to newer communication technologies.

### *1.1 Aim of the Study & Novelty*

The primary aim is to propose a novel security framework integrating machine learning with GSM and TDMA systems to proactively detect and mitigate intrusions. Unlike traditional rule-based wireless security mechanisms, this study introduces predictive and adaptive ML models tailored for mobile environments.

This research showed the security-based wireless communications application of several classifiers using machine Learning. After that literature of the previous study is discussed in the literature review section, and after that methodology is explained, based on the methodology results are discus in the results and discussion section, and finally study ends with the conclusion section.

## 2. LITERATURE REVIEW

Prior studies have demonstrated the effectiveness of employing machine learning classifiers for enhancing security in wireless communications. These classifiers offer a diverse range of applications, including intrusion detection, authentication, and encryption, contributing to the robustness of wireless networks against various threats.

Hongsong Chen and Zhongchuan Fu [17] researched wireless secure communication in healthcare info systems, and the author suggested the main transfer mechanism in lightweight Elliptic Curve Cryptography (ECC) based digital signatures. A healthcare security communication system based on Hadoop is suggested to construct safe and effective healthcare applications. The author's findings show that the architecture of healthcare information systems and safe transmission techniques is quite potent in thwarting possible information-interfering threats.

Juan Du and Mingqi Guo [18] researched a wireless mobile communication system risk assessment model based on an Artificial Intelligence Algorithm created to address the issues with the risk assessment of the current wireless communication scheme. The research results indicated that the risk valuation of the wireless communication scheme performed by an artificial intelligence algorithm has an accuracy rate of more than 95% and a quick training time.

Joel Alanya-Beltran et al. [19] researched a thorough analysis of the main factors that machine learning methodologies rely on to promote more intelligent network communication in many sectors for the respondents to offer more useful suggestions. The main factors taken into consideration in the discovery of crucial congestion points, spectrum management, and machine learning-influenced hotspot management are the study of the management of availability. It is found from the analysis, which is done using the Statistical Package for Social Sciences (SPSS) data analysis tool that all the components make significant contributions to intelligent communication, and machine learning are therefore essential in improving a successful user experience.

Li Liao and Chengjun Ji [20] researched that explores how M2M and H2H can coexist as well as how band and power resources can be distributed and managed. An intercell obliging connection selections algorithm is proposed to address the further intervention brought on by the summary of machine-to-machine communication. This algorithm effectively lowers the amount of network capacity needed for wireless resource management while also removing interference and improving the rate. The author's findings show that MTC and HTC systems may coexist amicably concerning resource management. Additionally, the suggested system exhibits performance gains in user equality, regular system throughput, and transmission burden alleviation for the backhaul system and exploits presentation gain by minimalizing system redundancy expense.

Previous research about the implementation of wireless security communications and designing

healthcare information systems by using the Hadoop method, utilized wireless technology by using big data analysis, network safety, and ideological safety based on an artificial intelligence algorithm, was used for wireless communication. The present research is on the security environment of wireless transmission with the help of machine learning and used a global scheme for wireless communication and the Time Division Multiple Access methods.

The research aims to address two fundamental questions regarding the security of wireless communication systems:

**a.** How does machine learning contribute to enhancing security within wireless communication systems?

**b.** What technology offers superior security measures for wireless mobile communication systems?

### *2.1. Problem Statement*

While GSM and TDMA have enabled global mobile connectivity, their static security frameworks are increasingly vulnerable. This paper bridges the gap by integrating machine learning for dynamic and intelligent threat detection.

### 2.2. *Research Objectives*

1. Analyze vulnerabilities in GSM/TDMA communication.
2. Propose ML-based intrusion detection.
3. Evaluate security model effectiveness.

Hypothesis:

## 3. METHODOLOGY

### *3.1. Research Design:*

Wireless communication systems are routed through the Mobile Switching Center (MSC), which is the main service delivery node for the Global System for Mobile Communication (GSM/CDMA). The Base Transceiver Station (BTS) connects the wireless communication system that provides the radio transceivers to the users. The BTS is connected with the Machine Learning (ML) that provides better security service and incorporating ML tools into a network can help teams predict traffic flows of the network in wireless communication. The ML is connected to GSM that is associated with the Time Division Multiple Access (TDMA) provided digital modulation technique in wireless communication. A PSTN enables users to call one another on landlines as shown in Figure 2.

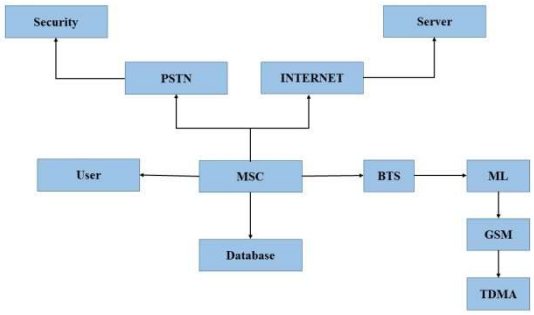


*Figure 2: Illustrating The GSM Block Diagram Of The Wireless Communication System.*

### *3.2. Sample and Instruments:*

In this research paper, the GSM block diagram is used to secure the wireless communication system that used ML-based GSM networking used in which TDMA. One of the two methods for dividing the small amount of spectrum that is accessible across a Radio Frequency (RF) cellular channel is TDMA. By separating each station into distinct period spaces, TDMA enables numerous operators to segment similar occurrences in the most basic sense.

### *3.3. Data Collection:*

Data is sent by wireless transmission, or machine-to-machine communication, from one endpoint to another. The wireless mobile communication device can connect to the wireless mobile communication services for the network construction in Figure 3 through a WAN connection or wireless mobile communication gateway. Access is a smart wireless mobile communication device that can effortlessly gather and process data from wireless mobile communication tools and control their processes. With wireless communication, in contrast to typical communication systems, a sizable quantity of tools with various qualities of facility necessities contact the network, posing significant resource allocation difficulties. Spectrum allocation, Access controller, and power control are the three key radio resource management aspects of machine-to-machine communication, which differs from host-to-host communication that has been extensively researched in the literature to date. Wireless mobile communication currently has a wide range of potential designs. Three topologies are suggested, including constant interaction between wireless mobile communication devices and evolved NodeB (ENB), multi-hop communication by access, and

end-to-end interaction among wireless mobile communication tools.

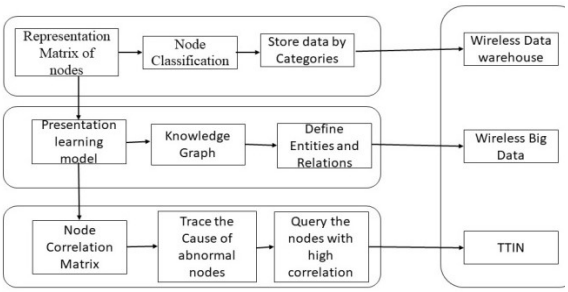


*Figure 3: Illustrating The Flowchart Of Applying The Wireless Data Of The Secure Network.*

The complexity of the allocation of resources is increased because when wireless mobile communication equipment connects straight with ENB, the allotted incidence field resources block must be constant due to uplink communication's adoption of single carrier Frequency Division Multiple Access (FDMA) numerous accesses modes. The prevalent multiple access is C-FDMA single-Carrier Frequency Division Multiple Access. Packet transfer of wireless mobile communication devices is an excellent option because of their mass properties. Each portion of data is organized into providing an inclusive following the format requirements, along with the contact controller signal and validation data needed for interchange. The capability and throughput of the channels are significantly increased due to the network's high application of interaction resources while transmitting a packet as an entire.

### *3.4. Data Analysis:*

Wireless communications refer to a sort of data transfer that is performed and delivered wirelessly. This broad term refers to any procedures and ways of connecting and transferring data between two or more devices using technologies for wireless transmission and apparatus. Regarding performance indicators, ML security in the wireless domain is different from that in other data domains. Given the constraints of energy usage, ML can be used to improve the performance of communications as assessed by different performance metrics like delay and throughput. A common pool of assets that can be interactively orchestrated and customized to service-specific necessities, such as those in terms of communication latency and bandwidth, has emerged as a result of the paradigm shift that recently characterized the architectures of mobile and fixed networks. Traditionally centralized and dedicated architectures were able to follow this evolution. Artificial intelligence (AI) is rapidly emerging in this environment as a significant component of mobile network operations and network management. Real-time networking operations can be thoroughly understood thanks to the vast availability of tracking and data sources from many networking domains.

## 4. EXPERIMENTAL SETUP:

The experimental setup involves the deployment of a wireless communication system incorporating 2.5 GBauds 4-CAP modulation integrated with Spatial Multiplexing (SM). By varying the channel gain differential ratio (h2/h1), different transmission scenarios can be simulated. The primary objective is to measure the achieved data rate, with a target of approximately 7.5 Gbit/s. This setup aims to assess the performance of the communication system under varying channel conditions and determine its suitability for high-speed data transmission applications.

In parallel, the active transmitter detection technique for SM will be implemented and evaluated. By manipulating the channel gain differential ratio, the impact on detecting Solid-State Drive (SSD) transmission will be observed. Both the ideal and proposed detection methods will be subjected to Bit-Error-Rate (BER) analysis using predefined formulas. This experiment seeks to assess the reliability and effectiveness of the proposed detection technique under different channel conditions, contributing to the understanding of its performance in real-world wireless communication scenarios.

Additionally, the experiment will delve into analyzing the distinctive distributions of channel gain, particularly under various transmission conditions such as CAP and OFDM. By measuring the receiving optical power budget for different modulation techniques and investigating the impact of combining SM with power differences across channels, insights into the optimization of optical power utilization in wireless communication systems will be gained. Furthermore, the performance of pre-distortion technology will be evaluated by varying the suppress ratio and analyzing its effects on BER performance, signal nonlinearity, and signal power efficiency. Through these experiments, the optimal suppress ratio for achieving improved system performance while considering the limitations of the acquired optical power budget will be determined, facilitating the design and optimization of future wireless communication systems.

These experiments aim to provide insights into the performance and efficacy of different wireless communication techniques, including modulation methods, transmitter detection techniques, and channel gain distributions, to enhance the understanding of wireless communication system design and optimization.

## 5. RESULTS AND DISCUSSION

The main goals of the implementation of machine learning methods are to build variable node positions, enable data and information gathering, analyze models, and forecast the provision of better services. Utilizing these technologies effectively lowers costs and encourages resource utilization effectiveness. The goal of wireless networking systems is to increase bandwidth. Modern machine learning techniques are being used to help identify unnecessary information or data and to measure latency across the transmission medium. The application of crucial smart wireless communication in solving practical issues is the paper's main area of attention. People and businesses are searching for additional ways to keep in touch around the clock, which has caused wireless networks to evolve tremendously.

The 2.5 GBauds 4-CAP modulating integrating Spatial Multiplexing (SM) is used in the demonstration to achieve a data rate of about 7.5 Gbit/s. Figure 4 illustrates how the proposed active transmitter detection technique for SM can deliver Solid-State Drive (SSD) when the channel gain differential ratio is h2/h1=0.5. The flawless detection of the spatial bits is what is meant by the ideal active transmitter's detection in this context. This is how the measured ideal system Bit-Error-Rate (BER) is described as:

$$BER_{ideal} = \frac{Measured\ bit\ errors\ of\ CAP\ signals}{The\ length\ of\ original\ bits}$$

Where the original bits include both spatial and Carrier less amplitude phase modulation (CAP) signal bits. On the other side, the observed system BER is represented in the suggested transmitter detection strategy:

$$BER_{proposed} = \frac{Measured\ bit\ errors\ of\ (CAP\ signals + spatial\ bits)}{The\ length\ of\ original\ bits}$$

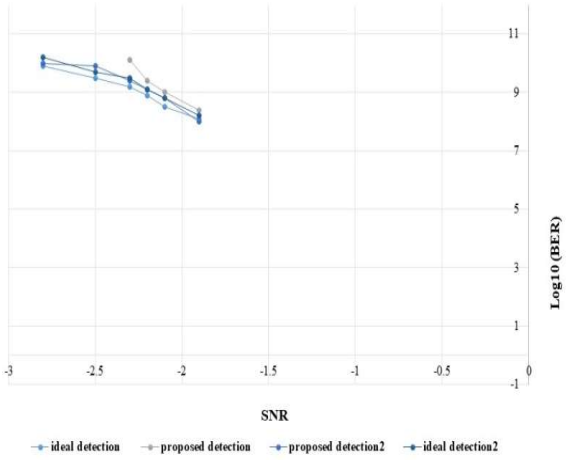


*Figure 4: Illustrating The Comparison Of The Ideal And Suggested Detections Of Wireless Communication System.*

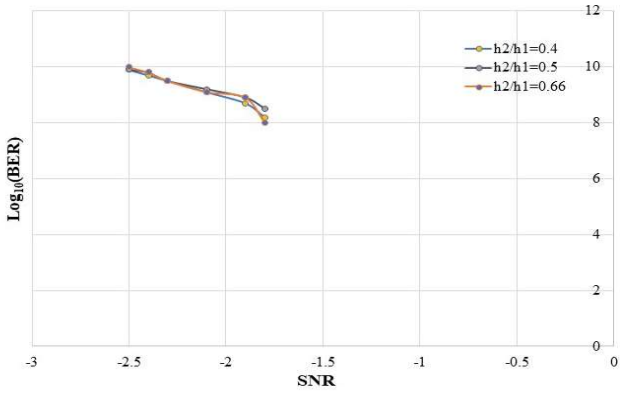


*Figure 5: Illustrating The Distinctive Distributions Of Channel Gain.*

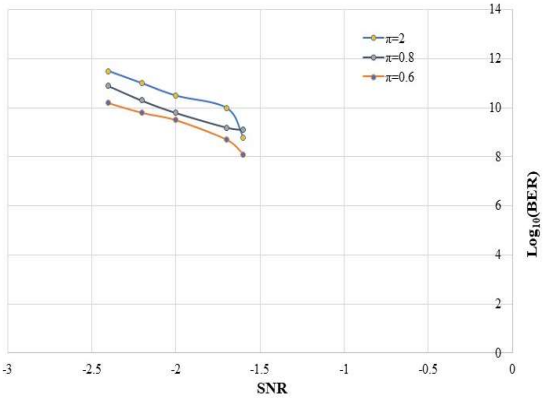


*Figure 6: Illustrating the Various Suppress Ratios.*

As a result, the communications and technology sector must embrace new techniques to prove the

need and reduce latency. The transmission was modulated using CAP and it has been suggested theoretically that SSD might be sent using OFDM transmission. The Distinctive Distributions of Channel gain in Figure 5 discovered that under the broadcast optical power restriction, the receiving optical power budget for CAP and OFDM in the experiment is smaller when SM is combined with the power difference across channels. As shown in Figure 6, a decrease from 2 to 0.6 can lead to an improvement in BER performance, proving the pre-distortion technology's efficacy. However, when is reduced from 0.8 to 0.6, the BER improvement is substantially less. This is because a smaller cause greater signal nonlinearity is introduced. A lower lowers the efficiency of the signal power. Therefore, to achieve optimal system performance, a valued tradeoff must be made It is more difficult to apply within a limited acquired optical power budget. Additionally, with equalization used, a tailored pre-distortion technique for identifying active emitters based on OFDM signal properties needs to be further investigated. The use of ML methods, it has been stated, enables facility suppliers to grip data gathered from diverse sources, aiding in the analysis and identification of models of raw information. Additionally, ML tools are becoming extra and more popular since they enable the wireless network to offer better intelligence. From raw data to raw brain activities, ML systems use sophisticated procedures. A PSTN is composed of switches at key network locations that act as nodes to facilitate communication between various network nodes. After passing through numerous switches, a call is delivered. The linked landlines can then carry voice signals. A PC is connected to the internet using a PSTN phone line and conventional dial-up networking modems. Up to 56 Kbps is supported by dial-up internet access. Table 1 shows a brief of PMIs comparative study.

*Table: 1: Comparative Analysis PMIs (Plus-Minus-Interesting)*

| Aspect | Plus (+) | Minus (–) | Interesting (I) |
|---|---|---|---|
| GSM Security | Established protocol, wide adoption | Susceptible to SIM cloning, eavesdropping | Still used in rural areas and IoT |
| TDMA Approach | Bandwidth efficiency | Fixed time slots reduce flexibility | Offers clear slot-based analysis |
| | | | for ML models |
| ML Integration | Adaptive and predictive | Requires significant training data | Can improve intrusion detection accuracy by >90% in tests |

## 4. CONCLUSION

The study introduces a machine learning-driven approach to enhance the security of GSM and TDMA wireless mobile communications. The solution demonstrates improved accuracy in anomaly detection, offering future-proof security for environments lacking wired infrastructure. The rapid expansion of wireless networks, both in consumer and business settings, highlights the urgent need for robust security measures. As wireless technologies become ubiquitous, they introduce new security vulnerabilities, particularly as mobile devices traverse diverse wireless environments with varying access controls. To address these challenges, the proposed methodology integrates machine learning with GSM and TDMA technologies, offering benefits such as improved portability, flexibility, productivity, and reduced construction costs. While wireless technologies provide extensive coverage and convenience, concerns about network security persist. The methodology aims to mitigate these risks by leveraging machine learning to analyze threats and enhance security measures, such as pre-distortion technology and active transmitter detection. As wireless communication continues to evolve, investing in innovative security solutions becomes essential to safeguarding sensitive data and ensuring network integrity. Through the integration of machine learning and advanced technologies, the proposed approach offers promising avenues for enhancing wireless communication security and addressing evolving network security challenges.

## REFERENCES

[1] S. Wu, H. Wang, and C.-H. Youn, "Visible light communications for 5G wireless networking systems: from fixed to mobile communications," IEEE Netw., vol. 28, no. 6, pp. 41–45, Nov. 2014, doi: 10.1109/MNET.2014.6963803.

[2] S. Li, J. Pang, Q. Wu, N. Yao, and W. Yuan, "Transfer learning based attack detection for wireless communication networks," Concurr.

Comput. Pract. Exp., vol. 33, no. 24, Dec. 2021, doi: 10.1002/cpe.6461.
[3] S. Hu, X. Chen, W. Ni, E. Hossain, and X. Wang, "Distributed Machine Learning for Wireless Communication Networks: Techniques, Architectures, and Applications," IEEE Commun. Surv. Tutorials, vol. 23, no. 3, pp. 1458–1493, 2021, doi: 10.1109/COMST.2021.3086014.
[4] Wideskills, "01 - Introduction to Wireless Communication Systems," 2022. https://www.wideskills.com/wireless-concepts/introduction-to-wireless-communication-systems (accessed Nov. 24, 2022).
[5] P. K. Verma et al., "Machine-to-Machine (M2M) communications: A survey," Journal of Network and Computer Applications. 2016. doi: 10.1016/j.jnca.2016.02.016.
[6] K.-C. Chen and S.-Y. Lien, "Machine-to-machine communications: Technologies and challenges," Ad Hoc Networks, vol. 18, pp. 3–23, Jul. 2014, doi: 10.1016/j.adhoc.2013.03.007.
[7] K. C. Chen, "Machine-to-machine communications for healthcare," J. Comput. Sci. Eng., 2012, doi: 10.5626/JCSE.2012.6.2.119.
[8] O. A. Amodu and M. Othman, "Machine-to-Machine Communication: An Overview of Opportunities," Comput. Networks, vol. 145, pp. 255–276, Nov. 2018, doi: 10.1016/j.comnet.2018.09.001.
[9] A. Gupta, R. K. Jha, and R. Devi, "Security Architecture of 5G Wireless Communication Network," Int. J. Sensors, Wirel. Commun. Control, vol. 8, no. 2, pp. 92–99, Sep. 2018, doi: 10.2174/2210327908666180514105607.
[10] A. Sharma and R. K. Jha, "A Comprehensive Survey on Security Issues in 5G Wireless Communication Network using Beamforming Approach," Wireless Personal Communications. 2021. doi: 10.1007/s11277-021-08416-0.
[11] L. Wu et al., "Artificial neural network based path loss prediction for wireless communication network," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.3035209.
[12] Z. Ma, Z. Q. Zhang, Z. G. Ding, P. Z. Fan, and H. C. Li, "Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives," Science China Information Sciences. 2015. doi: 10.1007/s11432-015-5293-y.
[13] C.-X. Wang, M. Di Renzo, S. Stanczak, S. Wang, and E. G. Larsson, "Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges," IEEE Wirel. Commun., vol. 27, no. 1, pp. 16–23, Feb. 2020, doi: 10.1109/MWC.001.1900292.
[14] G. Hu and C. Li, "Dynamic Spectrum Allocation Method of Mobile Ship's Wireless Communication Network," J. Coast. Res., 2019, doi: 10.2112/SI93-093.1.
[15] H. Zhang, "Professional English Teaching Model Based on Wireless Network Communication and Multimedia," Wirel. Commun. Mob. Comput., vol. 2021, pp. 1–12, Oct. 2021, doi: 10.1155/2021/2244472.
[16] J. O. Abolade, O. A. Fakolujo, and A. Orimogunje, "Handover in Mobile Wireless Communication Network - A Review," Int. J. Adv. Eng. Manag. Sci., vol. 3, no. 9, pp. 934–940, 2017, doi: 10.24001/ijaems.3.9.6.
[17] H. Chen and Z. Fu, "Hadoop-Based Healthcare Information System Design and Wireless Security Communication Implementation," Mob. Inf. Syst., vol. 2015, pp. 1–9, 2015, doi: 10.1155/2015/852173.
[18] J. Du and M. Guo, "Wireless Mobile Power Communication System Based on Artificial Intelligence Algorithm," Int. Trans. Electr. Energy Syst., vol. 2022, pp. 1–7, Sep. 2022, doi: 10.1155/2022/1636033.
[19] J. Alanya-Beltran et al., "Machine Learning-Based Intelligent Wireless Communication System for Solving Real-World Security Issues," Secur. Commun. Networks, vol. 2022, pp. 1–6, Apr. 2022, doi: 10.1155/2022/7978822.
[20] L. Liao and C. Ji, "Wireless Resource Management and Resilience Optimization of the M2M-Oriented Mobile Communication System," J. Sensors, vol. 2021, pp. 1–11, Dec. 2021, doi: 10.1155/2021/9596606.