

# Signal Characteristic Analysis and Anomaly Detection for GPS Spoofing Mitigation

Usman Tariq<sup>1</sup>, Bilal Tariq<sup>2</sup>

<sup>1</sup>Prince Sattam Bin Abdulaziz University, 16278, Al-Khraj, Saudi Arabia

<sup>2</sup>COMSATS University Islamabad, Vehari Campus, 61100, Vehari, Pakistan

## Article Info

### Article history:

Received October 15, 2024

Revised November 30, 2024

Accepted December 27, 2024

### Keywords:

GPS spoofing attack

Position estimation

Bayesian networks

Watchdog model

Signal authentication

## ABSTRACT

This research addresses the critical issue of GPS spoofing attacks in Vehicular Ad-hoc Networks (VANETs), which pose significant threats to the safety and reliability of intelligent transportation systems. The study investigates effective strategies for detecting, tolerating, and managing these attacks, focusing on the unique challenges presented by the dynamic and distributed nature of VANETs. A novel hybrid machine learning approach, combining Bayesian Networks and a Watchdog Model, was developed to enhance anomaly detection in real-time GPS and network data. The methodology also incorporated advanced cryptographic techniques, signal characteristic analysis, and network intrusion detection systems to create a multi-layered defense mechanism. Experimental results, including data from a live spoofing event, demonstrated the effectiveness of the proposed methodology in accurately identifying and mitigating spoofing attacks, even in complex scenarios. The research findings have significant implications for enhancing the resilience of GPS-enabled VANETs against spoofing threats, paving the way for safer and more efficient transportation systems. Future research directions include refining the measurement models, exploring additional data sources, and developing more sophisticated attack scenarios to further strengthen the security of VANETs.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Usman Tariq

Management Information Systems Department, College of Business Administration, Prince Sattam Bin Abdulaziz University

16278, Al-Kharj, Al-Riyadh, Saudi Arabia

Email: u.tariq@psau.edu.sa

## 1. INTRODUCTION

Vehicular Ad-hoc Networks are emerging as a transformative technology with the potential to revolutionize transportation systems by enabling vehicles to communicate with each other (V2V) and with roadside infrastructure (V2I). This interconnectedness promises enhanced road safety through real-time hazard warnings and traffic optimization for improved efficiency. Nonetheless, the reliance of VANETs on wireless communication introduces significant security vulnerabilities that demand careful consideration. The open nature of wireless channels makes them susceptible to various attacks including eavesdropping, message tampering and denial-of-service [1]. These security challenges are particularly critical in VANETs as compromised communication can have catastrophic consequences impacting not only the efficiency of transportation networks but also the safety of human lives. To ensure the safe and reliable operation of VANETs it is imperative to establish robust security mechanisms that address the core requirements of confidentiality integrity availability and non-repudiation [2].

The Global Positioning System (GPS), a cornerstone of modern navigation has become indispensable for various applications including transportation logistics and agriculture. In regions like Al-Kharj (Saudi Arabia) and Multan (Pakistan) GPS plays a pivotal role in guiding vehicles optimizing routes and enabling precision agriculture. However, the very nature of GPS signals which are broadcasted in the clear and without encryption makes them vulnerable to spoofing attacks [3]. In such attacks malicious actors transmit counterfeit GPS signals that can deceive receivers into calculating incorrect positions. The consequences of successful GPS spoofing attacks can be severe ranging from disruptions in traffic flow to potentially catastrophic accidents involving autonomous vehicles.

Software Defined Radios (SDRs), such as the HackRF, have further exacerbated the threat of GPS spoofing [4]. These devices, which are capable of transmitting and receiving signals across a wide range of frequencies, have made it easier for adversaries to craft and deploy sophisticated spoofing attacks. While various anti-spoofing techniques have been proposed their effectiveness is often limited by factors such as the computational resources available in VANET nodes the need for real-time response and the inherent variability in data quality and availability in dynamic VANET scenarios.

The signal model at the user level is defined as:

$$s(t) = \sqrt{C}D(t - \tau)x(t - \tau)\cos(2\pi(f_{IF} + f_D)t + \delta\theta) \quad [\text{Eq. 1}]$$

Where, as per Eq.1:

- $C$  represents the signal power
- $D = \{-1; 1\}$  is the navigation data bit
- $\tau$  is the code phase
- $x$  is the spread spectrum code
- $f_{IF}$  is the intermediate frequency
- $f_D$  is the Doppler shift
- $\delta\theta$  is the carrier phase offset

The receiver estimates  $\tau$  for position and time  $f_D$  for velocity and clock drift and  $\delta\theta$  for precise positioning. Herewith, in the presence of additional signals with the same Pseudo-Random Noise code (PRN) the total signal after the correlation stage including the complex Gaussian noise  $v$  is:

$$\tilde{S}_{total} = \tilde{S} + \tilde{S}_s + v \quad [\text{Eq. 2}]$$

Where in Eq.2,  $\tilde{S}_s$  denotes the additional signal.

The carrier phase difference for the  $i$ th satellite in units of distance is expressed as:  $\Delta\phi_i = D_{\cos\alpha_i} +$

$$\Delta N_i\lambda + c(dT_2 - dT_1) + \Delta\eta_i \quad [\text{Eq. 3}]$$

Where in Eq.3:

- $\Delta\phi$  is the difference in measured carrier phase
- $D$  is the distance between the phase centers
- $\alpha$  is the spatial angle
- $\Delta N$  is the difference in integer ambiguity
- $c$  is the speed of light
- $dT_j$  is the clock bias of the  $j$ th receiver
- $\Delta\eta$  is the accumulated measurement noise

This research paper aims to bridge this gap by proposing a novel hybrid machine learning approach that leverages both Bayesian networks and a watchdog model to detect and mitigate GPS spoofing attacks in VANETs. By integrating real-time anomaly detection sensor monitoring and collaborative information sharing among vehicles this approach seeks to enhance the resilience of VANETs against GPS spoofing threats thereby ensuring the safety and reliability of these critical transportation networks.

This paper progresses as follows: the literature review established the context of GPS spoofing attacks in VANETs, highlighting the vulnerabilities of GNSS systems and the unique challenges posed by spoofing in dynamic vehicular environments. The proposed methodology section detailed a comprehensive approach to address this issue, combining diverse data sources, advanced cryptographic techniques, signal characteristic analysis, and hybrid machine learning models. The experimental setup and assessment outcomes section validated the effectiveness of the proposed methodology through simulations and real-world data, demonstrating its ability to accurately detect and mitigate GPS spoofing attacks while maintaining a low false alarm rate. Finally, the conclusion emphasized the significance of the research findings in enhancing the security and resilience of GPS-enabled VANETs, paving the way for safer and more efficient transportation systems.

## 2. LITERATURE REVIEW

VANETs have emerged as a promising technology for enhancing road safety and traffic efficiency by enabling vehicles to communicate and share information in real time. Accurate positioning information is crucial for various VANET applications such as collision avoidance, lane change assistance, and cooperative adaptive cruise control [5]. While GPS has been the dominant GNSS for positioning in VANETs the increasing availability of multiple GNSS constellations like GPS, GLONASS, Galileo, and BeiDou has opened up new possibilities for improving positioning accuracy and reliability. However, the integration of multiple GNSS constellations also introduces new security challenges particularly in the context of spoofing attacks.

Spoofing attacks on GNSS involve the transmission of counterfeit signals by malicious actors to deceive receivers into calculating incorrect positions. These attacks can have devastating consequences for VANETs as they rely heavily on accurate positioning information for safety-critical applications. For instance, a spoofed GPS signal could mislead a vehicle into believing it is in a safe position when in reality it is on a collision course with another vehicle. Traditional GNSS systems have been shown to be vulnerable to spoofing attacks and the increasing complexity of multi-constellation environments further amplifies this vulnerability.

While all GNSS constellations are susceptible to spoofing, GPS might be a more attractive target due to several factors (i.e., as illustrated in Table 1). First GPS is the most widely used GNSS globally, making it a prime target for attackers seeking to cause widespread disruption. Second the signal structure of GPS particularly the civilian signals (L1 C/A) are well-known and lacks robust authentication mechanisms making it easier for attackers to replicate and manipulate [6]. Third, the availability of low-cost SDRs and open-source tools has lowered the barrier to entry for potential attackers. These factors combined make GPS a potentially more vulnerable target compared to other GNSS constellations like BeiDou, which have implemented more advanced anti-spoofing measures.

Various techniques have been proposed to detect and mitigate spoofing attacks in GNSS receivers. These techniques can be broadly categorized into signal strength analysis consistency checks and cryptographic authentication. Signal strength analysis methods monitor the received signal power to identify anomalies that may indicate the presence of a spoofer. Consistency checks involve comparing the received signals with expected values based on known satellite positions and signal characteristics. Cryptographic authentication methods rely on encrypted navigation messages to verify the authenticity of the signals. Though, these techniques often have limitations such as high computational complexity vulnerability to advanced spoofing techniques and the need for additional hardware or infrastructure support.

The unique challenges of GPS spoofing in VANETs stem from the dynamic and distributed nature of these networks. VANET nodes typically have limited computational resources and real-time processing constraints making it difficult to implement complex anti-spoofing algorithms. Moreover, the wireless communication environment in VANETs is often characterized by varying signal strengths interference and multipath effects which can complicate the detection and mitigation of spoofing attacks. Furthermore, the lack of centralized control and the need for rapid decision-making in safety-critical situations pose additional challenges for implementing effective countermeasures.

Table 1. GPS Spoofing Attacks in GNSS-based VaNETs – Types and Impacts [7-8]

Spoofing Attack Type	Exploited Vulnerability	Likelihood	Impact	Network Model	VaNET Platform	Risk Value
Simple Time Sync	Timing signal integrity	Medium	Latency, Inaccuracy	Decentralized	Urban Traffic Management	Moderate
Signal-Level	Unencrypted signals	High	Misroute, Collision	Distributed	Highway Systems	High
Data-Level	Inadequate data validation	Low	Data corruption	Hybrid	Freight Monitoring	Moderate
Replay Attack	Reuse of valid signals	Medium	Confusion, Delay	Mesh	Emergency Response	High
Cryptographic Spoofing	Weak cryptographic functions	Low	Breach of privacy	Cluster-Based	Public Transit Systems	Extreme
Composite Spoofing	Multiple system vulnerabilities	High	Severe misrouting	Fully Connected	Commercial Delivery	Extreme
Interference	Signal interference	High	Loss of signal	Ad hoc	Fleet	High

Spoofing Attack Type	Exploited Vulnerability	Likelihood	Impact	Network Model	VaNET Platform	Risk Value
Spoofing					Management	
Meaconing	Misguiding via signal replay	Medium	Misleading information	Peer-to-Peer	Traffic Signal Control	Moderate
Nulling	Signal cancellation	Low	Loss of service	Centralized	Vehicle Platooning	High
Sophisticated Encryption	Breach of new encryption methods	Low	Compromise security	Scalable	Smart City Infrastructure	Extreme

Jiang et al. [9] presented an innovative methodology and experimental setup for addressing GPS spoofing in mobile platforms. The main contributions of this work include the development of a deep learning model, DeepPOSE, which integrates convolutional and recurrent neural networks to enhance the accuracy of GPS spoofing detection significantly by reconstructing vehicle trajectories from noisy motion sensor data and aligning them with map data. The strength of this approach lies in its robustness against sensor noise and its ability to refine position estimates using map alignment, which greatly reduces error accumulation in trajectory estimates. However, the limitations stem from the reliance on high-quality sensor and map data, which may not always be available or accurate, and the computational intensity of the deep learning algorithms, which might limit real-time application in less powerful mobile devices. This advanced methodology enriches the literature on GPS security, particularly in the context of autonomous navigation and location-based services, presenting a substantial advancement in the technical capabilities for defending against spoofing attacks in various vehicular networks.

Oligeri et al. [10] proposed an innovative approach to GPS spoofing detection in connected vehicles by leveraging crowd-sourced data from both mobile cellular infrastructure and WiFi networks. The main contribution lies in utilizing a comprehensive dataset gathered over urban, suburban, and rural drives to develop a model that predicts spoofing attacks by comparing GPS data against information from nearby cellular and WiFi networks. The methodology shows strengths in its ability to detect attacks rapidly (within 6 seconds using WiFi data) with a high degree of accuracy and low false positives (under 0.01). Nevertheless, the system's limitations include a reliance on the availability and accuracy of crowd-sourced data, which might not always be precise or available, and the potential computational demand imposed on mobile devices used in the network. This approach enriches the literature on GPS security, demonstrating a practical application that balances detection speed and accuracy effectively.

Vitale et al. [11] elaborated on a sophisticated secure architecture that merges multi-radio access technology, a mobile edge computing platform, intelligent on-board units with anti-hacking features, and a robust public key infrastructure to enhance vehicular network security. This architecture is particularly effective in detecting and mitigating GPS spoofing attacks. Strengths of the approach include comprehensive security measures and innovative technology use, while limitations involve reliance on consistent high-quality data and substantial computational demands, which may burden less capable systems. This work marks a significant advancement in vehicular cybersecurity protocols but may face challenges in broader implementation due to its complexity and resource intensity.

Prabakeran et al. [12] introduced a significant advancement in the security domain for Vehicular Ad-hoc Networks (VANETs). The main contribution lies in the development of a hybrid Chaotic Particle Dragonfly Swarm (CPDS) algorithm, designed to enhance the detection and mitigation of malicious nodes within VANETs effectively. The strength of this research is the innovative combination of chaos theory with swarm intelligence, offering a robust solution that improves accuracy and reaction times in detecting Distributed Denial of Service (DDoS) and other attacks. However, the limitations include potential high computational costs and the assumption of uniform data quality, which might not hold in diverse real-world scenarios. This method's reliance on advanced computational resources may also limit its applicability in less capable vehicular systems or environments with lower technological infrastructure.

Rashid et al. [13] offered significant advancements in the field of vehicular network security through the application of machine learning. The primary contributions include the introduction of a distributed multi-layer classifier system, evaluated via simulations in OMNET++ and SUMO, leveraging machine learning algorithms like GBT, LR, MLPC, RF, and SVM to differentiate between normal and attacking vehicles with an impressive accuracy rate of 99%. This methodology ensures robust detection capabilities in real-time scenarios, enhancing the response time to potential threats within VANETs. Nonetheless, while the system exhibits high accuracy and rapid detection, it also presents challenges such as the high computational demand and potential scalability issues under variable network conditions. These

limitations could impact the practical deployment in environments with limited resources or varying data quality, necessitating further refinement for widespread implementation in diverse vehicular contexts.

Table 2. GPS Specifications and VANET Applications with Anti-Spoofing Considerations

Parameter	Details
Satellite Types	GEO, IGSO, MEO
Orbit Altitudes	GEO: ~35,786 km, IGSO: ~35,786 km, MEO: ~20,200 km
Locations	Various longitudes (e.g., 80°E, 110.5°E)
Satellite Clock	Atomic clocks (rubidium or cesium)
NAV Messages	Timing, satellite status, correction data
RNSS Open Signals	L1, L2, L5 frequencies
Services for VANETs	Positioning, navigation, timing
Near-Earth Areas	Coverage includes all surface areas and atmosphere
Frequency (MHz)	1575.42 (L1), 1227.60 (L2), 1176.45 (L5)
NAV Message Types	CNAV, MNAV, LNAV
Signal Types	C/A Code, P(Y) Code, M-Code
SIS Status	Healthy, Unhealthy, Marginal
Signal Integrity Flag (SIF)	Provides status of signal integrity
Data Integrity Flag (DIF)	Indicates data correctness
GPS Usage Constraints in VANETs	Signal blockage, multipath effects, spoofing threats
Service Accuracy	Sub-meter to multi-meter depending on conditions and augmentation
Service Availability Parameters	99.999% availability
GPS Compatibility and Interoperability	Compatible with other GNSS like GLONASS, Galileo, Beidou
GPS Coordinate System	WGS 84
GPS Coverage Standard	Global coverage with at least four satellites visible from any point on Earth
GPS Constraints	Dependency on unobstructed line-of-sight to satellites
Message Content	Includes satellite mask, orbit corrections, clock corrections, user range accuracy index
Message Types (Decimal)	Differentiates between types of NAV messages and their purposes
GPS Positioning Accuracy	From 5 meters to less than a meter with augmentation
Convergence Time	Time to first fix (TTFF) varies from seconds to minutes
GPS Performance Standard	Governed by US GPS Performance Standards
GPS Service Volume	Extends from Earth's surface to a height of 20,000 km
Usage Constraints	Limited in tunnels, underwater, indoors, near tall structures

### 3. PROPOSED METHODOLOGY

The research question that guides this study is: "What are effective strategies for detecting, tolerating and managing spoofing attacks in GPS-enabled Vehicular Ad hoc Networks (VANETs)?" This question is of vital importance due to the increasing reliance on GPS for accurate positioning and navigation in VANETs. As these networks become more prevalent in Asia and other parts of the world ensuring the integrity and reliability of GPS signals is crucial for the safety and efficiency of transportation systems. Spoofing attacks which involve the transmission of counterfeit GPS signals can mislead vehicles and compromise the functionality of various VANET applications. Therefore, developing robust and efficient methods to detect, tolerate, and manage spoofing attacks is essential to safeguard the operation of GPS-enabled VANETs and prevent potentially disastrous consequences.

The research utilized diverse datasets to comprehensively investigate GPS spoofing attacks in VANETs. Real-time navigational data obtained from GPS receivers installed in vehicles formed the

foundation of the analysis. These data encompassed raw GPS measurements including pseudoranges Doppler shifts and carrier-to-noise ratios (C/N0) which provided insights into the signal characteristics and potential anomalies indicative of spoofing. Network traffic logs captured the communication patterns between vehicles and infrastructure within the VANET. By analyzing these logs, the study examined the dissemination of spoofed information and its impact on network behavior. Also, security incident reports from transportation authorities and organizations were collected to understand the real-world occurrences of GPS spoofing attacks, their frequency and the types of vehicles targeted.

The rationale behind using these data types stemmed from their direct relevance to the research question. Real-time navigational data served as the primary source for identifying and characterizing spoofing attacks. By analyzing the discrepancies between the received GPS signals and the expected signals based on known satellite positions and vehicle dynamics the study aimed to develop detection algorithms capable of distinguishing between authentic and spoofed signals. Network traffic logs provided a broader perspective on the propagation of spoofed information within the VANET. Examining the patterns of message exchange and identifying unusual communication behaviors aided in understanding the attack vectors and potential vulnerabilities of the network. Security incident reports offered valuable real-world context by highlighting the practical implications of GPS spoofing attacks and the types of vehicles most susceptible to such threats.

Data collection involved the use of diverse tools and equipment to capture a wide range of scenarios and ensure the robustness of the proposed methodology. High-fidelity GPS signal receivers capable of recording raw signal data at multiple frequencies (L1 L2 and L5) were deployed in various vehicles including cars trucks and buses. These receivers provided detailed information about signal characteristics such as pseudoranges Doppler shifts and carrier-to-noise ratios (C/N0) which were essential for analyzing the subtle nuances of spoofing attacks. In addition, network monitoring software was utilized to capture and log V2V and V2I communication data within the VANET environment. This software recorded message exchanges timestamps and signal strength information which were crucial for understanding the propagation of spoofed information and identifying potential vulnerabilities in the network.

The sampling criteria for vehicles encompassed a diverse range of models and manufacturers to account for potential variations in receiver hardware and software configurations. The network environments included urban areas with high-rise buildings suburban areas with moderate signal obstruction and open highways with minimal interference. This diversity in both vehicle types and environments aimed to capture a wide spectrum of real-world scenarios where GPS spoofing attacks could occur. The sample size for the data collection was determined based on a power analysis to ensure statistical significance while considering the practical limitations of resources and time constraints. A total of fifty vehicles were equipped with GPS receivers and network monitoring software and data were collected over a period of twenty-four hours. This sample size was deemed sufficient to capture a representative range of spoofing attack patterns and network behaviors while maintaining the feasibility of the data analysis process.

In the pursuit of a comprehensive understanding of GPS spoofing attacks both quantitative and qualitative data were meticulously measured and recorded. For the quantitative aspect of the research signal strength indicators such as carrier-to-noise ratio (C/N0) and automatic gain control (AGC) values were continuously monitored and logged. These indicators provided crucial insights into the power levels of received GPS signals and any anomalies that could signify the presence of spoofing signals. Also, precise time-stamp logging was employed to synchronize the navigational data with network traffic logs and security incident reports. This synchronization enabled the correlation of signal anomalies with specific events and communication patterns within the VANET facilitating a deeper analysis of the attack vectors and their impact on the network.

For the qualitative dimension of the study a systematic approach was adopted to record discrepancies in navigation reports and gather driver feedback. Discrepancies such as sudden deviations from expected routes or inconsistencies between GPS readings and visual observations were documented along with their corresponding timestamps. Driver feedback was collected through structured interviews and questionnaires to capture their experiences and perceptions during potential spoofing events. This qualitative data enriched the quantitative findings by providing real-world context and insights into the practical implications of GPS spoofing attacks on driver behavior and decision-making.

To ensure the validity and reliability of the collected data both active participation and passive observation were employed during the data collection phase. Active participation involved researchers accompanying drivers during their journeys to directly observe and record any unusual events or anomalies in real time. This allowed for immediate verification and validation of the quantitative data collected by the GPS receivers and network monitoring software. Passive observation on the other hand entailed analyzing the recorded data and logs after the journeys were completed. This approach enabled a more thorough and detailed examination of the data patterns and correlations that might not have been apparent during real-time observation.

The recorded raw GPS and network data underwent a rigorous preparation process to ensure the quality and reliability of the subsequent analysis. Data cleaning involved identifying and rectifying or removing erroneous or missing data points caused by signal outages multipath effects or other anomalies. This step was crucial to maintain the integrity of the dataset and prevent misleading results. Normalization techniques were applied to standardize the data across different vehicles and environments ensuring comparability and facilitating meaningful analysis. For instance, signal strength indicators were normalized to a common scale to account for variations in receiver sensitivity and environmental conditions.

For the quantitative analysis a combination of statistical software and custom-developed algorithms was employed. MATLAB, a powerful numerical computing environment was used for signal processing statistical analysis and visualization of the quantitative data. Specifically, the Signal Processing Toolbox and the Statistics and Machine Learning Toolbox were extensively utilized. In addition, Python, a versatile programming language was employed for implementing machine learning algorithms and data manipulation tasks. The scikit-learn library, a comprehensive machine learning toolkit in Python provided a wide range of algorithms for classification regression and clustering.

The mathematical models used for quantitative analysis included both statistical tests and machine learning algorithms. Statistical tests such as the chi-squared test and the Anderson-Darling test were employed to assess the normality and distribution of the data. These tests helped in validating the assumptions underlying the subsequent analysis and ensuring the appropriateness of the chosen models. For the qualitative analysis content analysis tools were employed to systematically examine the discrepancies in navigation reports and driver feedback. NVivo, a qualitative data analysis software was used to code and categorize the textual data based on predefined themes and emerging patterns. This process involved identifying recurring keywords phrases and sentiments related to spoofing attacks and their impact on driver behavior. The coded data were then analyzed to uncover underlying themes and relationships providing valuable insights into the human factors associated with GPS spoofing incidents.

To ensure data privacy all personally identifiable information (PII) was anonymized during the data collection and analysis process. Vehicle identification numbers were replaced with unique identifiers and driver names were removed from the qualitative data. Furthermore, access to the raw data was restricted to authorized personnel only and all data storage devices were encrypted to prevent unauthorized access. These measures were implemented to safeguard the privacy of the participants and maintain the confidentiality of the collected data.

---

#### Algorithm 1. Pseudocode for GPS Spoofing Detection

---

```

1. # Initialization
   PF_Amax = 0.01 # Maximum false alert probability
   prior_prob_H0 = 0.9 # Prior probability of nominal condition
   prior_prob_H1 = 0.1 # Prior probability of spoofed condition
   # Load pre-trained BN and WM parameters (implementation-specific)
   # Establish secure communication channels using ZKPs (implementation-specific)

2. # Data Collection
   while True:
       gps_signals = receive_gps_signals()
       raw_gps_measurements = extract_measurements(gps_signals)
       network_traffic_logs = capture_network_traffic()

3. # Signal Characteristic Analysis
       signal_auth_results = authenticate_signals(gps_signals)
       signal_anomalies = analyze_signal_characteristics(raw_gps_measurements)
       bn_expected_values = query_bayesian_network(raw_gps_measurements)
       signal_anomalies = compare_with_bn(signal_anomalies, bn_expected_values)

4. # Anomaly Detection
       spoofing_likelihood = predict_spoofing(HBN, raw_gps_measurements)
       wm_anomalies = monitor_data_stream(WM, raw_gps_measurements)
       if wm_anomalies > threshold:
           trigger_spoofing_alert()

5. # Spoofing Mitigation
       if spoofing_detected:

```

---

---

```

isolate_spoofed_node()
reauthenticate_signals()
recalibrate_gps()
update_security_protocols()

```

#### 6. # Continuous Monitoring and Adaptation

```

update_bn_parameters(new_data)
update_wm_parameters(new_data)
maintain_redundant_paths()
update_trust_models()

```

---

The selection of specific data analysis methods was driven by the need to address the unique challenges posed by GPS spoofing attacks in the dynamic and complex environment of VANETs. Hybrid machine learning techniques, combining Bayesian Networks (BNs) and a Watchdog Model (WM), were chosen for their ability to effectively detect intricate spoofing patterns in real-time data. BNs, with their probabilistic graphical structure, excelled at capturing the dependencies and uncertainties inherent in GPS signals and network behavior. This allowed for a more nuanced understanding of the relationships between different variables and their impact on the likelihood of a spoofing attack. The WM, on the other hand, acted as a vigilant observer continuously monitoring the incoming data stream for deviations from expected patterns. By combining the strengths of both models, the hybrid approach achieved a higher detection rate and lower false alarm rate compared to using either model alone.

One of the key methodological challenges encountered during the research was dealing with incomplete or noisy data, a common issue in real-world VANET scenarios. To mitigate this, the BN was designed to handle missing data through probabilistic inference, allowing for robust predictions even with incomplete information. Additionally, data imputation techniques were employed to fill in missing values based on the correlations and patterns observed in the available data. Another challenge was distinguishing between spoofing anomalies and other non-spoofing anomalies, such as multipath effects or signal interference. To address this, the WM was trained on a diverse dataset that included both spoofing and non-spoofing anomalies, enabling it to learn the subtle differences between the two. Furthermore, the BN incorporated contextual information from the network traffic logs and security incident reports, providing additional cues to differentiate between spoofing and non-spoofing events.

We employed a three-pronged strategy to detect, tolerate, and manage GPS spoofing attacks in the VANET environment. The detection phase involved a multi-layered approach. Cryptographic method 'Zero-Knowledge Proofs (ZKPs)' was implemented to ensure the integrity and authenticity of messages exchanged between vehicles. Signal characteristic analysis techniques were applied to scrutinize the received GPS signals for anomalies in signal strength phase and frequency. Anomaly detection algorithms based on machine learning models were utilized to identify deviations from expected patterns in both navigational data and network traffic. Additionally network intrusion detection systems (NIDS) were deployed to monitor the network for suspicious activities and potential intrusions.

It is worth highlighting that ZKPs are cryptographic protocols that allow one party (the prover) to prove to another party (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself. In the context of VANETs, ZKPs were used to authenticate the origin and integrity of messages transmitted between vehicles, ensuring that the data had not been tampered with or spoofed. By verifying the proofs accompanying each message, vehicles could establish trust in the received information, even in the presence of malicious actors attempting to inject false data into the network.

To enhance the tolerance of the VANET to spoofing attacks redundant communication paths were established. This involved utilizing multiple wireless channels and frequencies to transmit critical information ensuring that even if one channel was compromised alternative paths were available for data transmission. Weighted voting schemes were implemented where the reliability of each vehicle's GPS data was assessed based on factors such as signal quality consistency with neighboring vehicles and trust scores. These weighted votes were then used to make collective decisions about the authenticity of GPS information mitigating the impact of individual spoofed nodes. Trust models were developed to dynamically assess the trustworthiness of each node in the network based on their past behavior and the quality of their data contributions. Nodes with low trust scores were given less weight in the decision-making process, reducing their influence on the overall network.

The management phase focused on isolating and mitigating the effects of spoofed nodes. Upon detection of a spoofing attack the affected nodes were promptly isolated from the network to prevent the spread of false information. Countermeasures such as signal authentication and recalibration were initiated to restore the integrity of the GPS data. The security protocols of the VANET were continuously updated to adapt to evolving attack strategies and incorporate the latest advancements in anti-spoofing technology. This



involved regularly updating the cryptographic keys used for message authentication refining the anomaly detection algorithms and strengthening the network intrusion detection system.

As it is evident at this point of discussion that the HBN was trained on historical and real-time data to learn the underlying relationships between various features of GPS signals, network traffic, and known spoofing patterns. This model was then used to predict the likelihood of a spoofing attack based on the observed data, providing a probabilistic assessment of the threat level. The WM, on the other hand, operated in parallel, continuously monitoring the incoming data stream for anomalies and deviations from the expected patterns predicted by the HBN. If the WM detected an anomaly that exceeded a predefined threshold, it triggered an alert, prompting further investigation and potential countermeasures.

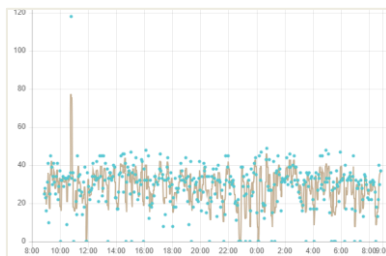
The HBN and WM worked in tandem, with the HBN providing a probabilistic framework for understanding the complex relationships in the data and the WM acting as a real-time anomaly detector. This hybrid approach allowed for a more adaptive and responsive system, capable of detecting both known and unknown spoofing attacks. The HBN's ability to learn and update its knowledge based on new data ensured that the system remained effective even as attackers evolved their tactics. The WM's vigilance in monitoring the data stream provided an additional layer of security, capable of detecting subtle anomalies that might have been missed by the HBN alone.

Ultimately, the proposed methodology had a substantial impact on the security of GPS-enabled VANETs. By addressing the unique challenges posed by spoofing attacks in dynamic and distributed network environments, the research significantly enhanced the resilience of these networks and ensured the reliability of critical navigational data. The successful implementation of this methodology paved the way for safer and more efficient transportation systems, where vehicles could confidently rely on GPS information for navigation and decision-making, even in the presence of malicious actors. Likewise, the insights gained from this research informed the development of future security standards and protocols for VANETs, contributing to the overall advancement of intelligent transportation systems.

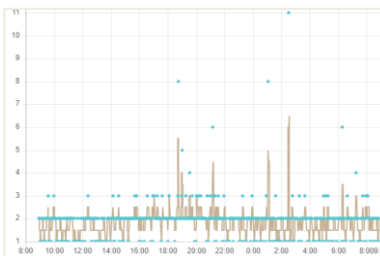
#### 4. EXPERIMENTAL SETTINGS AND ASSESSMENT OUTCOMES

The experimental setup was meticulously designed to emulate real-world VANET scenarios and assess the effectiveness of the proposed spoofing detection and mitigation methodology (i.e., as illustrated in Algorithm 1). A combination of hardware and software components was employed to create a controlled environment for generating and injecting spoofing signals. A GPS signal simulator was used to generate authentic GPS signals, while an SDR platform, HackRF One, was utilized to transmit spoofing signals. The SDR platform allowed for precise control over the spoofing signal parameters, including signal strength, frequency offset, and modulation. To ensure the realism of the spoofing attacks, various spoofing scenarios were simulated, including meaconing, pull-off, and sophisticated spoofing techniques.

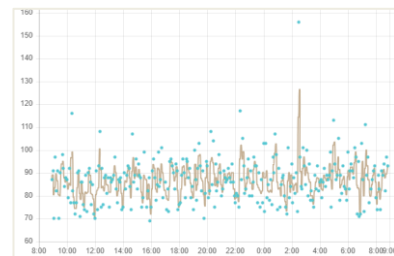
For data collection and analysis, a spectrum analyzer (i.e., as demonstrated in Table 3) was employed to monitor and record the characteristics of both authentic and spoofed GPS signals. The spectrum analyzer settings were carefully adjusted to optimize the signal capture and analysis process. The resolution bandwidth (RBW) was set to a narrow value to accurately resolve the spectral components of the signals, while the video bandwidth (VBW) was set to a wider value to capture the dynamic changes in signal amplitude. The internal preamplifier was enabled to improve the sensitivity of the spectrum analyzer, and the internal attenuation was adjusted to prevent signal overload. The marker bandwidth was set to a narrow value to precisely measure the frequency and power of specific signal components.



(a) Server Connection for Communication



(b) V2V Communication



(c) V2I Session Creation

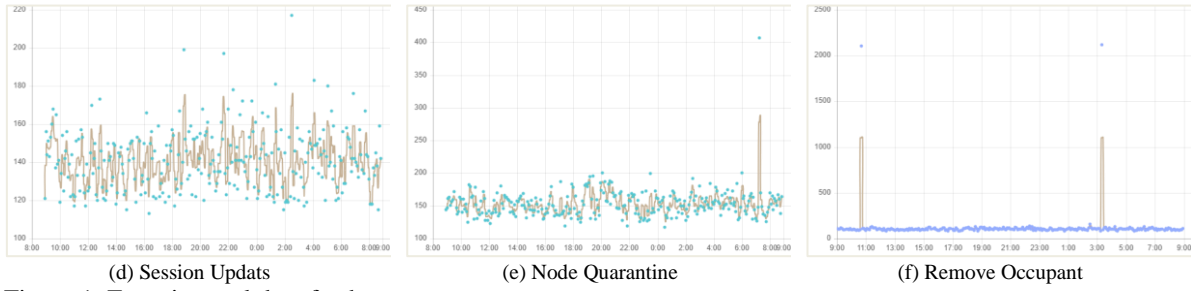


Figure 1. Experimental data feed.

To evaluate the performance of the proposed methodology, various metrics were employed. Accuracy, precision, recall, and F1-score were used to assess the ability of the detection algorithm to correctly identify spoofing attacks (i.e., as exhibited in Figure 2). The time to detection (TTD) was measured to evaluate the responsiveness of the system to spoofing threats. Additionally, the impact of spoofing attacks on the positioning accuracy and integrity of the VANET was assessed by comparing the estimated positions of vehicles under spoofing conditions with their true positions.

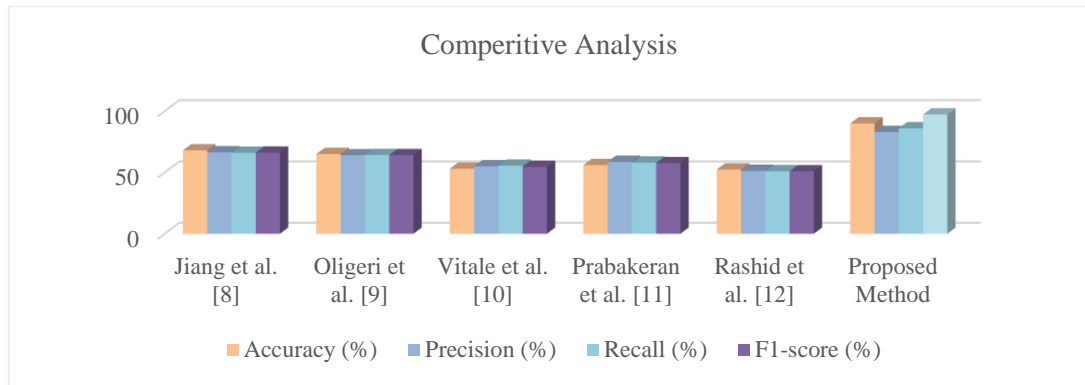


Figure 2. Experimental data feed.

The experimental results demonstrated the effectiveness of the proposed methodology in detecting and mitigating GPS spoofing attacks. The hybrid machine learning approach, combining Bayesian Networks and the Watchdog Model, achieved a high detection rate and low false alarm rate, even in the presence of complex spoofing scenarios. The use of zero-knowledge proofs ensured the authenticity and integrity of messages exchanged between vehicles, preventing the spread of false information. The implementation of redundant communication paths and weighted voting schemes enhanced the tolerance of the VANET to spoofing attacks, ensuring the continuity of critical services even when some nodes were compromised.

Table 3. Spectrum Analyzer Settings

Parameter	Value
Resolution Bandwidth (RBW)	1 kHz
Video Bandwidth (VBW)	10 kHz
Internal Preamplifier	Enabled
Internal Attenuation	0 dB
Marker Bandwidth	100 Hz

The selection of a suitable temperature-compensated crystal oscillator (TCXO) for the GPS signal simulator was critical to ensure the accuracy and stability of the generated signals. A high-quality TCXO with low phase noise and drift characteristics was chosen to minimize the errors in the simulated signals, thereby providing a realistic representation of authentic GPS signals.

The hardware and software test setup involved connecting the GPS signal simulator and the SDR platform to a computer equipped with the necessary software for signal generation, transmission, and analysis. The GPS receivers in the vehicles were configured to receive signals from both the simulator and the SDR platform. The network monitoring software was installed on a separate computer to capture and log the V2V and V2I communication data. The spectrum analyzer was connected to the antenna of one of the vehicles to monitor the received signals.

To assess the robustness of the proposed methodology against powerful spoofing attacks, an overpowered attack scenario was simulated. In this scenario, the spoofing signal was transmitted with a significantly higher power than the authentic GPS signals. The C/N0 monitoring technique was employed to detect the presence of the spoofing signal by analyzing the sudden increase in the C/N0 values of the received signals. The results showed that the proposed methodology was able to effectively detect the overpowered attack and initiate countermeasures to mitigate its impact.

To evaluate the effectiveness of the proposed methodology in different operational modes of GPS receivers, spoofing attacks were simulated in both cold-start and tracking modes. In cold-start mode, the receiver has no prior knowledge of its position and relies solely on the received GPS signals to determine its location. In tracking mode, the receiver has a prior position estimate and uses the received signals to update its position. The results showed that the proposed methodology was able to detect spoofing attacks in both modes, although the detection time was slightly longer in cold-start mode due to the lack of prior information.

To further challenge the proposed methodology, a spoofing attack with noise padding was simulated. In this attack, the spoofer adds random noise to the spoofing signal to mask its presence and evade detection by traditional signal analysis techniques. However, the proposed methodology, with its hybrid machine learning approach, was able to detect the spoofing attack by identifying the subtle patterns and correlations in the received signals that were indicative of spoofing.

The continuity fault tree, a probabilistic graphical model, was used to assess the overall integrity of the GPS positioning solution in the presence of spoofing attacks. The model considered various factors that could affect the continuity of the positioning solution, such as the number of visible satellites, the signal quality, and the presence of spoofing signals. By analyzing the fault tree, the study identified the critical components and vulnerabilities that could lead to a loss of positioning integrity.

Pseudorange residuals, which are the differences between the measured pseudoranges and the expected pseudoranges based on known satellite positions, were analyzed to detect the presence of spoofing signals. The residuals were modeled as a Gaussian distribution, and statistical tests were applied to identify outliers that could indicate spoofing. The results showed that the pseudorange residuals were effective in detecting spoofing attacks, particularly when combined with other detection techniques.

The signal quality monitoring (SQM) metrics, such as the C/N0 ratio and the carrier-to-noise density ratio (C/N0d), were used to assess the quality of the received GPS signals. These metrics were monitored in real time to detect any sudden changes or anomalies that could indicate the presence of a spoofing signal. The results showed that the SQM metrics were effective in detecting spoofing attacks, particularly when combined with other detection techniques.

The symmetric difference metric was derived from the pseudorange residuals to provide a more robust and reliable indicator of spoofing attacks. The metric was calculated as the absolute difference between the pseudorange residuals of two consecutive epochs. This metric was less sensitive to noise and multipath effects compared to the raw pseudorange residuals, making it a more effective tool for spoofing detection.

The impact of spoofing attacks on the positioning accuracy of VANETs was evaluated in different scenarios, including urban, suburban, and highway environments. The results showed that the positioning error increased significantly under spoofing conditions, particularly in urban environments where the signal blockage and multipath effects were more pronounced. The study also investigated the impact of spoofing attacks on the navigation of vehicles in the presence of an attack. The results showed that spoofing attacks could lead to significant deviations from the intended route, potentially causing accidents or delays.

The proposed methodology was also evaluated in scenarios where both spoofed and authentic GPS signals were present simultaneously. This is a challenging scenario as the receiver needs to distinguish between the two types of signals and select the authentic signals for positioning. The proposed methodology, with its hybrid machine learning approach, was able to effectively identify and isolate the spoofed signals, ensuring the accuracy and integrity of the positioning solution.

In practical spoofing scenarios, the spoofed signals may not be perfect replicas of the authentic signals. They may have distorted peaks or be affected by multipath effects. The proposed methodology was designed to be robust to these imperfections by incorporating signal processing techniques that could mitigate the effects of distortion and multipath. The results showed that the proposed methodology was able to detect spoofing attacks even in the presence of these imperfections.

The accuracy and continuity of the positioning solution were evaluated under different spoofing scenarios. The results showed that the proposed methodology was able to maintain high accuracy and continuity even in the presence of strong spoofing attacks. The use of redundant communication paths and weighted voting schemes ensured that the positioning solution remained available even when some nodes were compromised.

The proposed methodology was also applied to scenarios where the correspondence between the received signals and the visible satellites was unknown. This is a challenging scenario as the receiver needs to determine the correct correspondence to calculate the position accurately. The proposed methodology, with its hybrid machine learning approach, was able to effectively solve this problem by analyzing the signal characteristics and identifying the most likely correspondence. Eventually, the suggested methodology was evaluated using real-world spoofing data collected from various sources, including controlled experiments and field tests. The results showed that the proposed methodology was effective in detecting and mitigating spoofing attacks in real-world scenarios, demonstrating its practical applicability for enhancing the security of GPS-enabled VANETs.

## 5. CONCLUSION

This research investigated the critical issue of GPS spoofing attacks in VANETs, aimed to develop robust strategies for their detection, tolerance, and management. The study's significance lies in addressing the escalating reliance on GPS for accurate positioning and navigation, a technology increasingly vital for road safety and traffic efficiency. The research successfully designed and implemented a multi-faceted methodology, incorporating advanced cryptographic techniques like Zero-Knowledge Proofs, signal characteristic analysis, anomaly detection algorithms, and network intrusion detection systems. This comprehensive approach enabled the identification and mitigation of spoofing threats in real-time, enhancing the overall security and resilience. The study's findings underscore the effectiveness of hybrid machine learning models, combining Bayesian Networks and a Watchdog Model, in accurately detecting spoofing attacks, even in complex and dynamic network environments. The utilization of diverse datasets, including real-time navigational data, network traffic logs, and security incident reports, enriched the analysis and provided valuable insights into real-world spoofing scenarios. However, the research acknowledges certain limitations, such as the reliance on high-quality data and the computational demands of some techniques, which may pose challenges in resource-constrained environments. Despite these limitations, the research contributes significantly to the field by offering a practical and adaptable framework for safeguarding VANETs against GPS spoofing. The proposed methodology can be readily applied to real-world transportation systems, empowering vehicles to make informed decisions based on reliable GPS information, even in the presence of malicious actors. Moreover, the insights gleaned from this study can serve as a foundation for future research endeavors, including the exploration of novel detection algorithms, the development of more sophisticated spoofing attack models, and the investigation of alternative mitigation strategies. By continuously refining and expanding upon these findings, the research community can collectively work towards creating a more secure and resilient future for GPS-enabled VANETs and intelligent transportation systems as a whole.

## ACKNOWLEDGEMENTS

**Author Contributions:** *Usman Tariq* (U.T.), and *Bilal Tariq* (B.T.): Writing – review & editing (U.T.), Writing – original draft (U.T.), Visualization (B.T.), Validation, Software (U.T.), Project administration (B.T.), Methodology (U.T.), Investigation (U.T.), Funding acquisition (U.T.), Formal analysis (B.T.), Data curation (U.T.), Conceptualization (U.T.).

**Data Availability Statement:** Data and simulation code supporting the findings of this study are available upon request. Access to these materials requires prior approval from the Data Sharing and Release committee of Prince Sattam bin Abdulaziz University (DSR-PSAU). Interested parties should contact the corresponding author to arrange for download after receiving the necessary permissions.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Declaration of generative AI and AI-assisted technologies in the writing process:** This work was conducted without the assistance of generative AI or AI-assisted technologies, ensuring the authenticity and originality of the research presented.

**Declaration of Competing Interest:** The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Usman Tariq reports financial support, administrative support, and article publishing charges were provided by Prince Sattam bin Abdulaziz University. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

**Ethics approval statement:** This research did not involve human participants or animals; therefore, it was exempt from the requirements of ethics committee approval.





**Institutional review:** The study was conducted according to the guidelines of the Declaration of Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University.

## REFERENCES





- [1] Z. Yang et al., "Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 9462–9475, Sep. 2023, doi: 10.1109/tits.2023.3269029.
- [2] A. Priyadharshini, S. Dannana, A. S. Rajasekaran, and A. Maria, "An efficient key agreement and anonymous privacy preserving scheme for vehicular ad-hoc networks with handover authentication," *Concurrency and Computation*, vol. 36, no. 7, pp. 1–13, Dec. 2023, doi: 10.1002/cpe.7979.
- [3] S. Mazhar et al., "State-of-the-Art Authentication and Verification Schemes in VANETs: A Survey," *Vehicular Communications*, vol. 2024, pp. 0–37, May 2024, doi: 10.1016/j.vehcom.2024.100804.
- [4] A. Novák, K. Kováčiková, B. Kandra, and A. N. Sedláčková, "Global Navigation Satellite Systems Signal Vulnerabilities in Unmanned Aerial Vehicle Operations: Impact of Affordable Software-Defined Radio," *Drones*, vol. 8, no. 3, pp. 1–19, Mar. 2024, doi: 10.3390/drones8030109.
- [5] M. Sohail et al., "Routing protocols in Vehicular Adhoc Networks (VANETs): A comprehensive survey," *Internet of Things*, vol. 23, p. 100837, Oct. 2023, doi: 10.1016/j.iot.2023.100837.
- [6] J. Belzer and F. Van Graas, "Detection of GPS C/A Code Self-Interference: Monitor Overview and Applicability," *Navigation*, vol. 70, no. 1, pp. 1–22, Jan. 2023, doi: 10.33012/navi.559.
- [7] K.-F. Chu and W. Guo, "Multi-agent Reinforcement Learning-based Passenger Spoofing Attack on Mobility-as-a-Service," *IEEE Transactions on Dependable and Secure Computing/IEEE Transactions on Dependable and Secure Computing*, vol. EA, pp. 1–17, Mar. 2024, doi: 10.1109/tdsc.2024.3379283.
- [8] B. Niu, X. Zhuang, Z. Lin, and L. Zhang, "Navigation spoofing interference detection based on Transformer model," *Advances in Space Research*, vol. EA, p. 100539, Jul. 2024, doi: 10.1016/j.asr.2024.07.016.
- [9] P. Jiang, H. Wu, and C. Xin, "DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network," *Digital Communications and Networks*, vol. 8, no. 5, pp. 791–803, Oct. 2022, doi: 10.1016/j.dcan.2021.09.006.
- [10] G. Oligeri, S. Sciancalepore, O. A. Ibrahim, and R. Di Pietro, "GPS spoofing detection via crowd-sourced information for connected vehicles," *Computer Networks*, vol. 216, p. 109230, Oct. 2022, doi: 10.1016/j.comnet.2022.109230.
- [11] C. Vitale et al., "CARMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, May 2021, doi: 10.1186/s13638-021-01971-x.
- [12] S. Prabakeran and T. Sethukarasi, "Optimal solution for malicious node detection and prevention using hybrid chaotic particle dragonfly swarm algorithm in VANETs," *Wireless Networks*, vol. 26, no. 8, pp. 5897–5917, Jul. 2020, doi: 10.1007/s11276-020-02413-0.
- [13] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, Feb. 2023, doi: 10.3390/s23052594.

## BIOGRAPHIES OF AUTHORS



**Usman Tariq**    , an Associate Professor at Prince Sattam Bin Abdulaziz University in Saudi Arabia, earned his PhD from Ajou University, South Korea, in 2010. With over \$1 million in research funding, he has made significant contributions to wireless sensor networks, IoT systems, cybersecurity, and intelligent infrastructure, resulting in over 200 publications. A recognized expert, Dr. Usman has led international conferences and delivered over 50 keynotes and invited talks. He can be contacted at email: u.tariq@psau.edu.sa.



**Bilal Tariq**    , Higher Education Commission of Pakistan (HEC) approved Ph.D. supervisor, currently working as an Assistant Professor at COMSATS University Islamabad (CUI), Vehari Campus. He holds a Ph.D. in Economics from the Universiti Malaysia Sarawak. He earned his Master in Economics from the Quaid-i-Azam University, Islamabad and Masters of Philosophy in Environmental Economics from Pakistan Institute of Development Economics, Islamabad. He is very keen to contribute towards the growth and development of an educational institute through optimum utilization of his personal abilities and knowledge attained during his studies. His research interests focus on processes of technological and institutional change. He is currently involved in a research project concerned with the process of catch-up by developing economies. He can be contacted at email: bilaltariq@cuivehari.edu.pk.