Journal of
Sensor and Actuator Networks

MDPI

Article

Detecting and Localizing Wireless Spoofing Attacks on the Internet of Medical Things

Irrai Anbu Jayaraj, Bharanidharan Shanmugam *, Sami Azam and Suresh Thennadil

Energy and Resources Institute, Faculty of Science and Technology, Charles Darwin University, Darwin, NT 0810, Australia; j.irraianbu@gmail.com (I.A.J.); sami.azam@cdu.edu.au (S.A.); suresh.thennadil@cdu.edu.au (S.T.)

* Correspondence: bharanidharan.shanmugam@cdu.edu.au

Abstract: This paper proposes a hybrid approach using design science research to identify rogue RF transmitters and locate their targets. We engineered a framework to identify masquerading attacks indicating the presence of multiple adversaries posing as a single node. We propose a methodology based on spatial correlation calculated from received signal strength (RSS). To detect and mitigate wireless spoofing attacks in IoMT environments effectively, the hybrid approach combines spatial correlation analysis, Deep CNN classification, Elliptic Curve Cryptography (ECC) encryption, and DSRM-powered attack detection enhanced (DADE) detection and localization (DAL) frameworks. A deep neural network (Deep CNN) was used to classify trusted transmitters based on Python Spyder3 V5 and ECC encrypted Hack RF Quadrature Signals (IQ). For localizing targets, this paper also presents DADE and DAL frameworks implemented on Eclipse Java platforms. The hybrid approach relies on spatial correlation based on signal strength. Using the training methods of Deep CNN1, Deep CNN2, and Long Short-Term Memory (LSTM), it was possible to achieve accuracies of 98.88%, 95.05%, and 96.60% respectively.

Keywords: IoMT; wireless spoofing; Deep-CNN; Hack RF; software defined radio

Citation: Jayaraj, I.A.; Shanmugam, B.; Azam, S.; Thennadil, S. Detecting and Localizing Wireless Spoofing Attacks on the Internet of Medical Things. *J. Sens. Actuator Netw.* **2024**, *13*, 72. https://doi.org/10.3390/jsan13060072

Academic Editor: Lei Shu

Received: 12 August 2024
Revised: 8 October 2024
Accepted: 16 October 2024
Published: 1 November 2024

1. Introduction

The Internet of Things (IoT) technologies have revolutionized the healthcare industry, leading to the concept of the Internet of Medical Things (IoMT). The healthcare industry is becoming increasingly aware of potential cyber threats [1], with spectrum security being a significant challenge for organizations [2]. Spectrum security is identifying, analyzing, and responding to threats posed by radio signals to networks. With the rise of connected and IoT devices, the healthcare industry is more vulnerable than ever to the threat of spectrum attacks [3]. This paper addresses the vulnerability of IoMT networks to spectrum attacks, where malicious actors exploit radio signals to compromise data security and patient care. Key challenges are spectrum security (identifying and mitigating threats posed by radio signals to IoMT networks), data security (protecting sensitive patient data transmitted by IoMT) and Trustworthiness (ensuring the integrity and authenticity of data within the IoMT ecosystem). While solutions exist for data security within IoMT, they do not fully address spectrum security threats (target identification and localization). This paper proposes a novel approach using RF (radio frequency) spectrum signal analysis to address the emerging security concerns in the IoMT landscape.

IoMT spectrum signal analysis involves the examination of electromagnetic signals emitted by various IoMT devices. These signals carry valuable information about device operation, communication protocols, and potential vulnerabilities. By employing signal analysis techniques, anomalies detection and deviations from normal device behavior can be detected, aiding in the identification of malicious activities, unauthorized access, and data breaches. IoT localization refers to determining precisely where a device is in

the IoT network based on the information it contains [4]. Localization is important in enhancing the security and safety of IoMT spectrums. Precise location tracking plays a vital role in security applications like intrusion detection system (IDS) [5] and access control in the spectrum layer. Locating unauthorized devices or monitoring potentially hazardous equipment in real-time can prevent accidents and security breaches. When the objective is to localize all the devices, it is referred to as IoT network localization. Various technologies, such as GPS, wireless communication signals, and sensor data, can be utilized for this purpose. In the context of IoMT localization, deep learning can be employed to analyze data from multiple sources, thereby improving the accuracy and reliability of position predictions [6,7]. However, there is no cost-effective software defined radio (SDR) with deep learning and localization methods in the security ecosystem landscape [8,9]

The attacks of this nature can compromise the confidentiality, integrity, and availability of sensitive patient data, leading to serious consequences such as misdiagnosis, incorrect treatment, and even harm to the patient. IoMT devices operating under a Machine Implantable Communication System (MICS) are highly vulnerable to sniffing attack frameworks [10]. The existing research review examines how IoMT devices can be compromised by layered attacks, attacks against protocols, sniffing attacks, security test beds, deep learning, and data collection. In addition, IoMT devices that lack RF SDR security can also be compromised by physical attacks, and intruders can gain access to the devices and tamper with them, potentially causing harm to the patients. These attacks can sometimes disrupt critical medical sensors, leading to life-threatening situations [11].

To solve the above problem, this research aims to develop a hybrid two module approach to identify the threats. This research offers two significant contributions in the field of IoMT. This study contributes to the scientific landscape by introducing innovative approaches that have not been employed in IoMT spectrum security research before. Through these pioneering contributions, this research not only expands the boundaries of knowledge but also lays a foundation for future advancements in the IoMT cybersecurity spectrum field and cognitive spectrum security domain.

1.1. Existing Gaps

There is a challenge in distinguishing between legitimate and rogue transmissions when detecting and localizing wireless spoofing attacks in radio frequency-based IoMT environments. A growing number of frameworks exist along with low-cost software defined radio [12], but there is a lack of comprehensive frameworks capable of dealing with single-node and multi-node spoofing scenarios while ensuring the confidentiality and integrity of sensitive medical information.

1.2. Contributions

- Novel Framework for Spoofing Attack Detection:

A novel framework that utilizes the spatial characteristics RSS and uses Deep-CNNs for robust RF transmitter classification. Additionally, this paper presents DADE and DAL frameworks implemented on Eclipse Java platforms for localizing RF source targets. In IoMT environments, this hybrid approach improves the framework's ability to differentiate legitimate from rogue devices, identifying the localization and addressing both single-node and multi-node spoofing scenarios.

- Integration of Elliptic Curve Cryptography (ECC):

As part of the framework, Elliptic Curve Cryptography (ECC) is also integrated to ensure the confidentiality and integrity of sensitive IoMT data. Advanced deep learning techniques combined with robust encryption methods enable this framework to detect and localize spoofing attacks and ensure that critical information is protected within IoMT networks.

The remainder of this paper is organized as follows: In Section 2, the most recent works are discussed. In Section 3, the proposed bi-module framework is presented (Module

1—DADE and DAL framework; Module 2—ECC and RFDL in DSRM). In Section 4, the experimental specifications are highlighted that are related to our RFDL workflow. The results of the experiments are discussed and analyzed in detail in Section 5. The final section, Section 6, concludes with a discussion of future work.

2. Related Works

Over the last few years, the received signal strength indicator (RSSI)-based localization method has gained popularity due to the availability of low-cost SDR receivers. In contrast, receivers with GPS, a disciplined oscillator, and a wider bandwidth are more costly than those described [13]. It has been demonstrated in [14,15] that SDR receivers can be used to perform RF fingerprinting and localization. An RSS-based localization system for IoMT RF security requires a low-cost Raspberry Pi or RTL-SDR to be practical and usable.

This problem has been addressed by proposing a bias reduction algorithm for RSSI-based localization [16]. The proposed algorithm demonstrates promising results in improved localization accuracy, enhanced robustness to environmental factors, and reduced errors. The paper reports that the proposed bias reduction algorithm effectively reduces the bias, thus significantly enhancing the localization accuracy of the system. While the paper's approach is novel and can potentially improve RSSI-based localization, some limitations should be considered. Furthermore, the authors do not compare their approach to other bias reduction methods, which may have yielded better results. Despite these limitations, the paper presents a valuable contribution to RSSI-based localization and highlights the importance of practically validating proposed algorithms.

The study by [17] investigates methods for improving the accuracy of a practical system for localizing sources based on the Time Difference of Arrival (TDOA). The paper provides a detailed description of how this can be achieved and reports numerical results obtained from real-world experiments that demonstrate the effectiveness of the proposed method. Their methodology is comprehensively described, and numerical results obtained from real-world experiments illustrate the effectiveness of their approach. Overall, the paper thoroughly investigates methods for improving the accuracy of a TDOA-based source localization system. The study by [18] investigates K-means algorithm that assigns data points to clusters and updates the cluster centers. K-means clustering is a partition-based algorithm that groups data points into clusters based on similarity. By evaluating the sum of squares within each cluster, the elbow method helps identify the optimal number of clusters. In this article, K-means is applied to assign data points to the closest cluster centers after extensively evaluating both methods. In the second step, K-means updates the cluster centers. This process is repeated until the algorithm converges and the clusters that it finds are stable. One of the advantages of K-means is that it can cluster data with any number of dimensions. Overall, Ref. [19] presents a clear and concise description of the research problem, the proposed solution, and the experimental results in collecting RF fingerprinting data from Hack-RF devices. However, the paper could benefit from additional details about the experimental methodology, such as the size and characteristics of the dataset used, the types of deep learning algorithms that can be employed and recommended architectures, and the choice of specific key performance indicators (KPIs) used to identify the performance of the proposed solution.

This study uses a deep learning model that is not explicitly described. Despite this, it is stated that Keras is used as the front end and TensorFlow as the back end for running all experiments [20]. Moreover, the study proposes to use deep learning over raw I/Q data for radio fingerprinting. In the paper, future research directions are suggested, including combining deep learning with other deep-learning approaches or exploring other transfer learning techniques. All environments showed a 63.31% improvement in target localization when using k-nearest neighbor algorithms (k-NN) and maximum likelihood estimation (MLE). A clear description of the method, results, and future implications of the proposed method is provided in this research. Unlike the SDP-MLE method, the proposed method did not suffer from poor geometry between the target and receivers. However, it did

not compare the proposed method with other advanced techniques, so it was difficult to evaluate its performance against existing techniques. In addition, the paper lacks detailed information about the experimental methodology, such as setup, receiver number, frequency range, and other important parameters. It is also not mentioned whether the reported results are statistically significant nor how the performance improvement was evaluated. Lastly, a hybrid approach using Deep CNN was proposed, but no further details were provided.

An overview of the literature discusses a technique for identifying IoT-accessing devices to prevent system intrusion. It mentions that while the proposed method shows promising results in detecting rogue devices, it lacks a real-world evaluation and was tested in a controlled laboratory environment [21]. The complexity of IoT networks and potential interference from other wireless networks were not considered. Further research is needed to evaluate the technique's effectiveness in more realistic network environments. However, experimental results indicate that it can identify rogue devices with 95% accuracy in a real-world application. In this paper, a new technique using neural networks (NN) and deep neural networks (DNN) is proposed to detect rogue radio frequency transmitters [22] and classify [23] trusted ones more accurately. The paper acknowledges limitations including relying on known transmitters and suggests future work to enhance the approach, like exploring other deep learning techniques and combining them with RF fingerprinting. It presents a new method using GANs to identify rogue RF transmitters and classify trusted ones. However, the paper could be improved by addressing the mentioned issues, discussing related work, describing the experimental setup, analyzing the results more thoroughly, and considering limitations and future possibilities. Existing solutions for RF data security in IoMT radio frequency networks are limited, and therefore the proposed hybrid approach is necessary. Even though current methods protect data transmission, they do not fully address vulnerabilities related to spectrum security in terms of classification, identification, localization, and mitigation. There are several critical issues that result from this. Threats that are unknown: Existing solutions might not detect malicious radio signals that attempt to intercept or manipulate data within the IoMT network by intercepting or manipulating its radio signals. There is a potential risk of compromised patient care because of unresolved spectrum security threats. Spectrum security threats may result in the exposure of sensitive IoMT data, potentially impacting the privacy of patients as well as their health outcomes.

As a result, our study aims to fill the gap in current IoMT security by focusing on spectrum security to identify the source target and localize the source of the threat. By implementing ECC in the IQ fingerprints, we are ensuring data security as well as the identification of rogue transmitters. Deep CNN on the IQ RF fingerprinting dataset from the Hack RF device is presented to classify the rogue transmitters. Furthermore, we implemented the DADE and DAL frameworks presented in the Section 3 to detect and localize attacks. All of this was conducted in a design science research methodology, allowing us to create a hybrid approach that provides unified visibility of threat management in the RF ecosystem of the IoMT. The Hack RF is an open-source, low-cost, and programmable software-defined radio—a device that can measure and sample wireless signals, allowing us to detect and classify rogue transmitters. The IQ RF fingerprinting dataset is our primary data source for this experiment. In our study, we have included Supplementary Materials that can be accessed at the supplementary section. The data contains information about the frequency, signal strength, and signal type of the transmitter as well as many other parameters. There are several challenges that need to be overcome to implement this proposed study. *The complexity of radio frequency signal analysis:* The analysis of radio frequency signals to detect and localize threats requires advanced signal processing techniques and encryption techniques to be used. Therefore, we employed advanced ECC techniques to encrypt generated fingerprints from the Hack-RF signals we received. *Integrated with existing systems:* It is important for the proposed approach to integrate seamlessly with the existing IoMT business infrastructure without disrupting the existing cybersecurity

management system architecture. The software as a service microservices using a React framework, tailwind user interface, authentication using Firebase, a cloud-based database using the Firestore, and a payment gateway through Stripe as a minimum viable product (MVP) were in the roadmap.

There are a few data security solutions within IoMT, but they mainly focus on mechanisms of encryption and access control that are used to protect data during transmission in the IoMT infrastructure development phase. There are, however, some limitations to these solutions. They are limited in their scope because they do not address the security concerns posed by malicious radio signals that target the communication spectrum directly. In addition, the collected spectrum is not encrypted to prevent RF poisoning attacks from occurring. In addition to the vulnerabilities inherent in the existing solutions, there are new attack methods such as spoofing and RF fingerprinting attacks as well as covet communication channels that exploit weaknesses in the transmission or reception of radio signals to exploit the weaknesses of the entire system.

Due to these limitations, it is necessary to take a hybrid approach that encompasses both the security of data as well as the security of the spectrum. This paper also makes significant contributions to the IoMT spectrum using the DADE and DAL framework, experimenting with our proposed method, and comparing its performance. The signal flow in the RF ecosystem shown in Figure 1 is vulnerable in either Bring Your Own Device (BYOD) or on-premises IoMT devices [24,25]. In the RF IoMT physical spectrum ecosystem, threats emerge through signals reconnaissance in open-source signal intelligence, recognition, modulation, classification, and localization of the signal target and are analyzed through a spectrum analyzer for further vulnerability. An RF-based system must be designed with various security measures to detect and prevent spoofing attacks in addition to risk evaluation and mitigation strategies [26]. To facilitate this process, we developed a hybrid approach with a Deep CNN to identify and localize the unauthorized SDR Hack-RF transmitters. Full detail is explained in the Section 3.

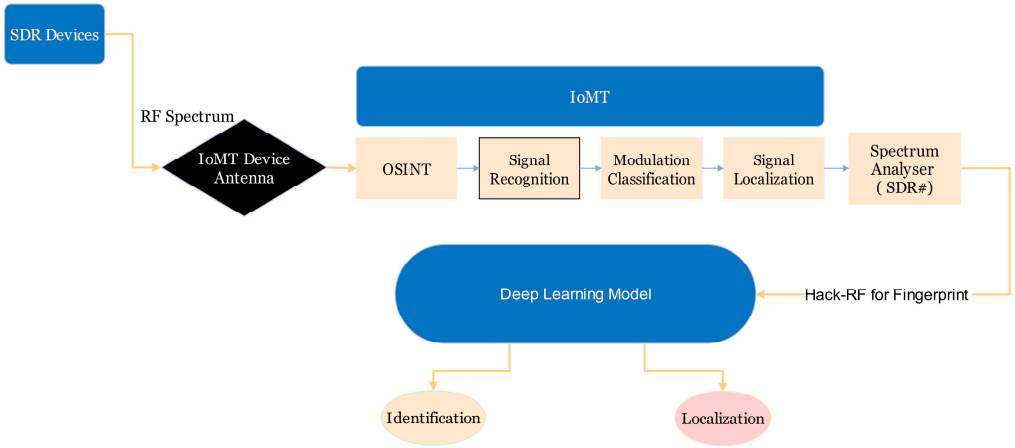

Figure 1. Generic signal flow for identifying RF imperfection characteristics.

3. Methodology

This study presents a novel multi-tier module framework that includes IQ fingerprint encryption, a DADE attack detection system, a DAL attack localization system, and a Deep CNN for RFML to enhance spectrum security and prevent side-channel attacks. In this study, a new methodology for RF fingerprinting and transmitter localization based on deep learning is introduced. The focus is on utilizing deep learning algorithms to harness the distinctive RF characteristics of wireless devices. This approach facilitates the accurate identification and classification of devices as well as generates unique fingerprints. By using deep learning in this context, RF-based localization and fingerprinting techniques may become more accurate and efficient. This approach enables the fast identification of devices within a network and detection of any malicious activity. Moreover, the localization

of rogue transmitters is of utmost importance for maintaining the security of the IoMT in the healthcare industry.

Figure 1 depicts a deep learning model for fingerprint recognition using software defined radio (SDR).

SDR Devices: The Hack RF functions as software-controlled radios that can transmit or receive radio signals across a wide range of frequencies.

IoMT Device/OSINT/Signal Recognition: This section refers to the stage where the Hack RF device receives signals emitted by various Hack RF devices in the IoMT devices' spectrum range. OSINT (Open-Source Intelligence) involves identifying the specific signal patterns from the received data based on publicly available information about the expected signals.

Modulation Classification: Modulation refers to the process of adding data to a carrier signal for transmission. Different modulation techniques encode data in various ways, and this classification helps to understand the format of the captured signal. The modulation techniques are AM (Amplitude Modulation), FM (Frequency Modulation), PM (Phase Modulation) for analog and ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying), PSK (Phase Shift Keying), and QAM (Quadrature Amplitude Modulation) for digital modulation.

Signal Localization (SDR): We determine the location of the Hack RF device though a hybrid approach explained in the Section 3.

Deep Learning Model: A deep learning model, specifically a Convolutional Neural Network (CNN), is employed to analyze the IQ fingerprint data. Fingerprint data refers to the unique characteristics extracted from the received Hack RF signal.

Identification/Localization: The deep learning model then performs two main tasks.

Identification: It attempts to identify the specific IoMT device frequency that transmitted the signal by analyzing the fingerprint data.

Localization: It also estimates the location of the IoMT device frequency based on the captured signal. The fingerprint characteristics of these signals are then analyzed using a deep learning model to identify the specific IoMT device and its location. This approach offers a potential solution for securing IoMT networks by recognizing authorized devices and identifying potential threats.

3.1. Module 1—DADE and DAL Framework

The DAL is developed to identify the localization of adversaries. The DAL system detects both attacks and the precise location of multiple opponents, even when they change their positions and techniques. This is accomplished using a combination of RSS and beacon-based techniques. DADE helps detect attacks before they can be damaged, while DAL helps localize the attackers and take appropriate actions. These two techniques can help keep networks and devices safe from malicious actors. To help mitigate the threat of spoofing attacks, researchers have developed many methods to detect them. One such method involves the detection phase, which includes two processes: constructing the network and calculating Euclidean distance. The process of constructing the network involves drawing the nodes using their dimensions. Each node is then connected, forming a network. This process is essential, as it transfers data between the nodes. The next process involved in the detect phase is calculating Euclidean distance. This consists of determining the distance between every two nodes. By calculating this distance, it is possible to detect attackers in the spectrum network. These two processes are essential to the detection phase of spoofing attacks, as they help identify attackers promptly. As such, researchers should be aware of the importance of these processes and how they can be used to detect attackers in a network. Researchers can better protect their IoMT networks from malicious actors by understanding the detection phase of spoofing attacks [27]. This work provides valuable insight into developing reliable detection, localization system frameworks, and prediction frameworks to identify the unauthorized SDR in a network.

The encryption of IQ fingerprint data protects users' data and prevents malicious actors from accessing it. In contrast, the DSRM-based attack detection framework identifies and detects potential attacks in the IoMT devices that use RF to transmit data between peers. DAL provides real-time monitoring and detection of malicious activities, and RFML provides spectrum security and side-channel mitigation. The proposed framework has been validated through simulations and Java test-bed experiments. IoMT security is demonstrated to be robust with the proposed framework. In addition, the proposed framework can also detect and localize the attack sources, thereby helping to reduce the impact of malicious activities. Encryption techniques, DADE, and DAL are combined in the proposed framework to provide spectrum security for IoMT data while detecting and localizing attack sources. Therefore, this work contributes a great deal to the secure management of IoMT data in the healthcare sector. Our approach involves implementing a DADE and DAL framework, as depicted in Figure 2 and Appendix A. Appendix A describes experiments and validations on the DADE and DAL modules. It consists of six phases: A.1 spoofing attack detection, A.2 received signal strength vectors, A.3 cluster analysis, A.4 attack number detection, and A.5 detection and localization frameworks.

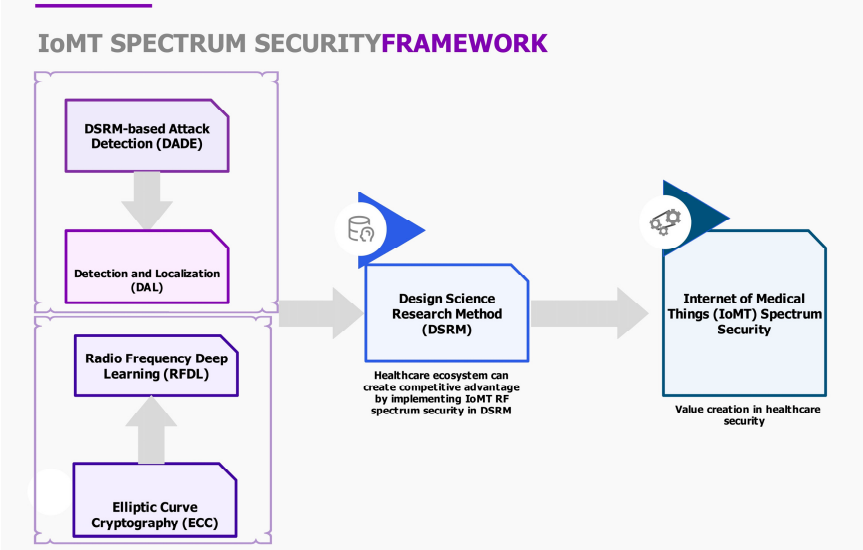

Figure 2. IoMT RF security framework.

3.2. Module 2—ECC and RFDL in DSRM

Design science research methodology (DSRM) helps create and refine solutions (artifacts) to address real-world problems. Through a cyclical process, DSRM involves identifying the problem, designing the artifact, evaluating its effectiveness, and then refining the solution based on the findings. This iterative approach aims to develop useful artifacts that improve a specific domain and design the overall system architecture and develop the necessary components. This includes designing algorithms for RF fingerprinting, signal localization, and integrating deep learning techniques into the system.

The modular design allows each component, such as Deep CNN and ECC encryption, to be integrated independently, providing flexibility in system architecture and simplifying updates while enabling future scalability. Using efficiency optimization techniques like model pruning and quantization, resource-heavy models can be deployed on resource-constrained IoMT devices without sacrificing performance because they reduce computational load. As a result of combining encryption and detection frameworks, enhanced security is provided against vulnerabilities that single-method solutions may miss, strengthening system resilience in sensitive environments.

The automation of testing and integration pipelines using DevOps and AI-driven automation streamlines the maintenance of complex systems, reducing the risk of fail-

ures during updates. Additionally, knowledge sharing and open-source resources lower expertise barriers, making it easier for organizations to upskill their employees or adopt pre-trained models and frameworks, thereby reducing their dependence on external consultants. The hybrid system's long-term scalability outweighs its initial complexity, as it is seamlessly integrated with IoMT networks, incorporating advanced security and detection without requiring significant re-engineering, making it future-proof and adaptable.

3.2.1. Step 1

The Internet of Medical Things (IoMT) has revolutionized healthcare, enabling remote patient monitoring, real-time data acquisition, and enhanced medical interventions. However, these interconnected devices and sensors introduce new vulnerabilities, attracting malicious actors who can exploit them for various purposes. Among these threats, wireless spectrum spoofing attacks pose a significant risk to patient safety and healthcare privacy. A literature review [27] examined wireless spectrum attacks and the potential impact of IoT (Internet of Things) on healthcare. By following the preferred reporting items for systematic reviews (PRISMA) guidelines [28], the authors conducted a thorough search for peer-reviewed articles on Scopus, PubMed, and Web of Science. A thorough review of professional academic research included impacts, layered attacks, attacks on protocols, sniffing attacks, field experiments with cybersecurity, deep learning, and data collection as well as an assessment.

3.2.2. Step 2

In the second step of DSRM, In-Phase Quadrature (IQ) data were collected from one receiver and five transmitters. The receivers and transmitters were Hack-RF Ones (with ANT500 antennas) running with GNU Radio [29]. Data at 2.45 GHz were collected at 2 MHz bandwidth and 2 MHz sampling rate. A total of three transmissions were collected for each transmitter, and 30 s were allowed between each transmission. The data were collected before and after the FFT and Wi-Fi Frame Equalizer. The current experiments utilized only I/Q data after a frame equalizer. A total of 32 K datasets were collected for each transmitter, of which 16 K were single carrier signals and 16 K were two carrier signals. To determine the transceivers' performance, the data were analyzed. In DADE and DAL RF frameworks, cluster analysis using medoid algorithm [30] plays an important role and is explained in the Appendix A.

3.2.3. Step 3

As part of the third step of DSRM solutions, we aimed at improving on the existing solution and presenting it as an artifact. In this process, the core behavior and structure of the artifacts are deduced, which help develop original artifacts to identify each SDR module from a pool of in a network and design science research methodology. This system is designed to use IQ fingerprinting data from the Hack-RF device. We implemented the ECC and RFDL module, as depicted in Figure 2. An Internet of Medical Things (IoMT) and Deep Convolutional Neural Network (CNN) are proposed for increasing spectrum security and preventing side-channel attacks. Multiple convolutional layers are used in the extraction process. A pooling layer, like max pooling, is used to reduce data size while preserving important information. Dropout regularization randomly drops a portion of neurons during training to prevent overfitting. To improve the network's convergence speed and performance, batch normalization layers are added. During the training process, the network's weights are fine-tuned by an optimizer. To measure the difference between predicted labels and actual labels, a suitable loss function, like categorical cross-entropy, is used. IQ fingerprint data are fed into the CNN model through RF signals transmitted by IoMT devices and encrypted using the proposed IQ fingerprint encryption technique. Encryption protects user data and prevents unauthorized access. These fingerprints are analyzed by the model and a classification result is generated. This result is used to determine whether the received RF signal originated from a legitimate IoMT device or if it originated

from a potential attacker. By filtering out malicious RF signals, this classification capability is instrumental in improving spectrum security and preventing side-channel attacks.

The various data extraction processes are as follows. *Data preprocessing and cleaning:* This initial stage focuses on preparing the RF IQ data model ingestion by eliminating irrelevant or missing data and ensuring uniform formatting of the dataset. *Data split:* The dataset is divided into a training set and a test set. The training set is utilized to train the model, while the test set serves to assess the model's performance. Feature selection and *hyperparameter tuning:* Relevant features are chosen from the dataset to for the model's learning process, while hyperparameters are fine-tuned the model performance. Model training: The model is trained using the training data, with its parameters continuously adjusted to refine its performance on the training set. Performance evaluation: The model's performance is gauged using the test set, measuring its efficacy in predictions. Evaluation metrics such as the F1 score provide insight into the model's effectiveness in classification tasks. The detailed deep CNN data extraction process architecture is shown in the Figure 3.

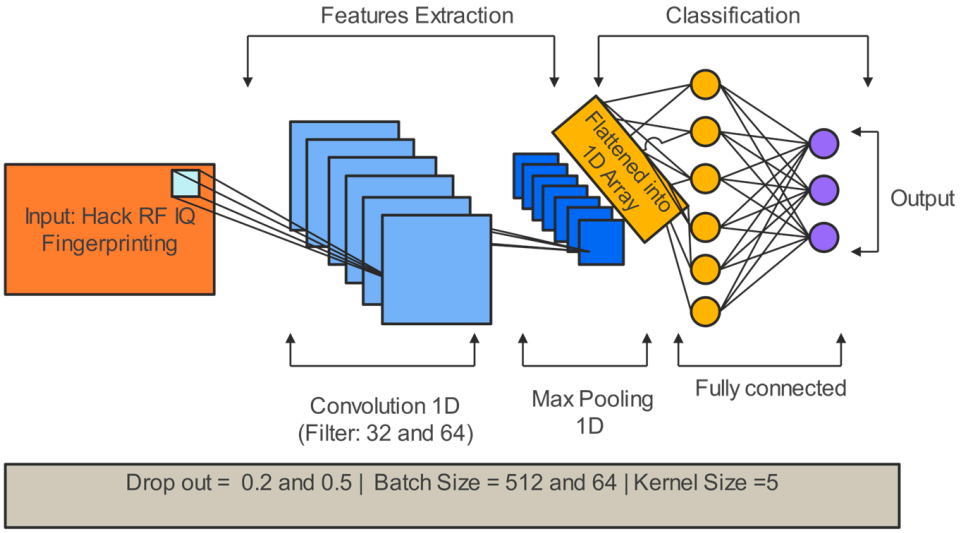

Figure 3. Deep CNN data extraction process.

To train the neural network model, the following hyperparameters are tuned as shown in Table 1. By randomly deactivating neurons during training, a dropout rate of 0.2 prevents overfitting. The number of samples processed in each training iteration is determined by the batch size, specified as five, which affects the efficiency of weight updates. The kernel size is five, which determines how much feature extraction occurs in convolutional layers. A neural network undergoes forward and backward passes with 2 epochs, affecting its convergence and learning abilities. A progress bar can be displayed during training in the verbosity mode, denoted as one, so training dynamics can be monitored in real-time. These hyperparameters are important in configuring the training process and shaping neural network performance.

Table 1. Summary of the hyperparameters used in the model training process.

Hyperparameter	Value	Description
Dropout	0.2/0.5	Rate of dropout applied to prevent overfitting during training.
Kernel Size	5	Size of the kernel used in convolutional layers.
Batch Size	512/64	Number of samples propagated through the network during each training.
Epochs	2/15	Number of times the entire training dataset is passed forward and backward through the neural network.
Verbose	1	Verbosity mode training.

Deep neural networks (CNNs) employ various layers such as batch normalization, max pooling, flattening, dense, and dropout layers, meticulously arranged using TensorFlow's library to accomplish the IQ classification tasks shown in Table 2. Initially, the input layer is void of filters and units, serving as the entry point; the next two layers employ1D convolutions with different filter counts (32 and 64) and Leaky ReLU activation, tasked with extracting features from the inputs. Each layer is followed by a batch normalization layer, which enhances model stability and efficiency. By strategically placing a 1D max pooling layer with a pool size of two, computational complexity is reduced and salient features are preserved.

Table 2. Deep CNN classification report.

Metrics	Precision (%)	Recall (%)	F1 (%)
Class 0 authorized transmitter	99	97	98
Class 1 unauthorized transmitter	99	100	99
Accuracy	99	98	99
Macro Avg	99	99	99

MaxPooling1D: This is a 1D max pooling layer that down samples the input along the temporal dimension by selecting the maximum value. A ReLU activation layer is added. As a next step, a flattening layer reshapes the output into a 1D vector, preparing it for the dense layers, which include two units with ReLU activation, capable of learning intricate data patterns and presenting higher-level features. Following the dropout layer is a deactivation layer that removes neurons selectively during training, mitigating 20% dropout rates. Lastly, the output layer culminates the architecture by providing binary classification probabilities via one neuron with activation. Using Mean Square Error (MSE) loss, Adam optimizer, and accuracy metric, the model is meticulously designed for optimization and evaluation.

3.2.4. Step 4

In the last step of design science research methodology, the evaluation process is carried out to analyze the success criteria of the proposed solutions against the findings or results [31]. This process involves observing and measuring how supportive the artifacts are toward solving the problems. In other words, we compare the objectives of the proposed solutions with the experimental findings through the demonstration process to improve the efficiency of the artifacts and communicate the results for further scope. The model is evaluated, and the F1 score is measured, combining precision and recall and a classifier's overall accuracy [32]. The area under the receiver operating characteristic (ROC) curve is also a measure of accuracy. It is used to measure the trade-off between true and false positives.

4. Experiment

In this study, we present the identification and testing of a Rogue SDR module in a spectrum network utilizing the Hack RF dataset as shown in Figure 4 [33]. The device specs of the SDR module include a frequency range of 1 MHz to 6 GHz, with a maximum sample rate of 20 MSPS and a resolution of 8 bits. The RF input power range is −5 dBm to 15 dBm, while the dynamic range of ADC/DAC is 48 db. The Rogue SDR module can operate from −40 °C to 85 °C and has a power consumption of 300 mA at 5 V, with a USB 2.0 interface. To conduct the testing, we utilized the Great Scott Gadgets ANT500 telescopic antenna, which is primarily designed for use with SDRs. The antenna has a frequency range of 75 MHz to 1 GHz and measures 16 inches (40.64 cm) when fully extended and 4.5 inches (11.43 cm) when collapsed. It has a male SMA connector with an impedance of 50 Ohms and a maximum power rating of 10 W. The higher-level goal is to identify any SDRs behaving abnormally, causing interference. The transmitted data from multiple radio nodes were collected using a reconfigurable radio's receive chain in IQ

format in a laboratory environment to achieve this. The next step involved measuring and studying RF fingerprinting features such as IQ imbalance, DC offset, and noise level [34]. This project's software requirements include using the Windows 11 operating system and Python programming language, with the Anaconda Navigator-Spyder 3 v5 as the front end. The Alienware m15 system has a 6-core Intel Core i 78750H CPU @ 2.20 GHz processor and 12 logical processors (s), 1 TB, a Logitech mouse, and a keyboard with 110 enhanced keys. These specifications will ensure that the software runs smoothly and efficiently for any higher load on the hardware.

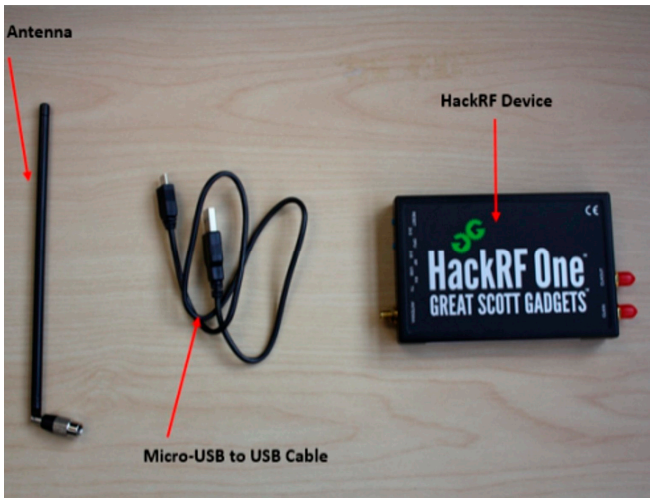

Figure 4. Hack RF device setup.

5. Results and Discussions

We proposed a hybrid approach to identify the rogue transmitter and classified it using Deep CNN1, Deep CNN2, and LSTM with accuracies of 98.88%, 95.05%, and 96.60%, respectively. We included the localization of the target with DADE and DAL RF frameworks, ECC encryption of Hack RF data, and experimental studies through a design science approach. To classify the rogue transmitters, we used a Deep CNN algorithm [35], which is a Convolutional Neural Network (CNN) type that can learn complex patterns from input data. The IQ RF fingerprinting dataset is trained and used to classify rogue transmitters. The results of our experiment showed that the Deep CNN1 could accurately classify rogue transmitters with an accuracy of more than 98.8%, as shown in the benchmarking report in Figure 5 and Tables 2 and 3. In evaluating the model's predictions, accuracy serves as a commonly employed metric, calculated by dividing the number of correct predictions by the total predictions. Table 3 shows the CNN classification benchmarking table where support is not provided for the methods GAN and KNN-MLE. According to the table, the proposed method performs better than other methods when comparing accuracy. The 98.8% F1 score indicates high accuracy in classifying IQ fingerprint data, demonstrating the effectiveness of the proposed method. The proposed method is more accurate than the other methods in the table, even though they also exhibited good F1 scores. Prediction performance is primarily measured by accuracy. A percentage (%) is used to denote the value of classified events. Ideally, a classification accuracy of close to 100% would result in more accurate results.

$$\text{Accuracy} = \text{TP} + \text{TN} \tag{1}$$

The F1-score is calculated by taking the harmonic mean of the precision and recall for each model and then summing them together. The F1-score measures the accuracy of the testing process. To calculate the average, precision and recall sets are used. This equation can be expressed as follows:

$$\text{F1 Score} = 2 \times \text{Precision} \times \text{Recall} \tag{2}$$

The recall calculates and predicts how many positive classes there are in the overall set of positive instances [36]. Precision computation determines how many positive classes represent a truly positive outcome [37].

In multi-class classification scenarios, macro-averaging and weighted averaging are two approaches for computing an average evaluation metric across all classes. Macro averaging assigns equal weights to each class, while weighted averaging accounts for the relative frequency of each class in the Weighted Avg of the data. The F1-score offers a comprehensive performance measure for each class, ranging from 0 to 1, with perfect precision and recall achieving a value of 1. Euclidean distances [38] are calculated in Table 4 and RSS vectors in Table 5.

$$d = \sqrt{[(x2 - x1)^2 + (y2 - y1)^2]} \quad (3)$$

x1 and y1 are the coordinates of the first point.
x2 and y2 are the coordinates of the second point.
$\sqrt{}$ is the the square root function.
d is the Euclidean distance between (x1 and y1) and (x2 and y2)

We selected the Euclidean column from the dataset and plotted the distribution of the values using a trend chart in Figure 5. The trend represents the frequency of different Euclidean.

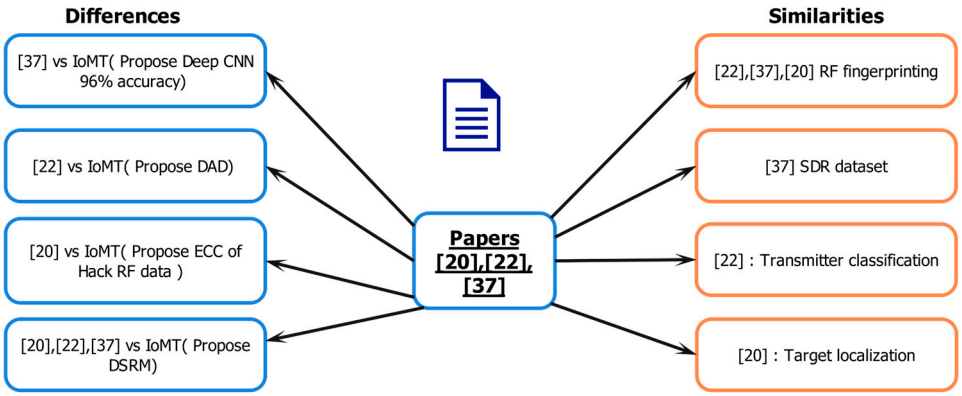

Figure 5. Benchmarking report [20,22,37].

The Table 3 presents the performance metrics of the Deep-CNN classifier in distinguishing between authorized and unauthorized transmitters. The classifier performs well across both classes and is highly accurate. For Class 0 (authorized transmitters), the precision is 99%, which means that out of all instances predicted as authorized transmitters, 99% are accurate. The recall is 97%, which indicates that out of all actual authorized transmitters, 97% were correctly identified. An F1 Score of 98% indicates a balanced performance in identifying authorized transmitters based on precision and recall. The precision of Class 1 (unauthorized transmitter) is 99%, which indicates that out of all instances predicted as unauthorized transmitters, 99% were correct. Among all actual unauthorized transmitters, 100% were successfully identified as such. Based on the harmonic mean of precision and recall, the F1 Score is 99%, which indicates an extremely accurate ability to identify unauthorized transmitters. 98.88% of the predictions made by the model have been correct, indicating a high degree of accuracy. The macro average values of precision of 99%, recall of 98%, and F1 score of 99% provide a balanced evaluation of each class performance due to its macro average values of precision of 99%, recall of 98%, and F1 of score 99%. In terms of precision, recall, and F1 score, the weighted average values are 99%, 99%, and 99%, respectively. These values provide a performance measure that considers class distribution as well. By examining these metrics, we can demonstrate the Deep CNN classifier's capability of distinguishing between authorized and unauthorized transmitters accurately, thereby demonstrating its reliability to perform this classification task.

Table 3. Benchmarking table.

Method	Precision (%)	F1(%)
CNN [37]	99	98
GAN [22]	99	99
KNN-MLE [20]	99	99
Deep-CNN1—Proposed	98.88	98.88
Deep-CNN2—Proposed	95.05	95.05
LSTM—Proposed	97.06	96.6

Also, Table 3 presents a comprehensive comparison of various methods in terms of precision and F1 scores, evaluating their performance. Among the established methods, CNN [37], GAN [22], and KNN-MLE [20] demonstrate consistently high performances, with all achieving precision scores of 99% and F1 scores ranging from 98% to 99%. In addition, novel approaches are presented, including Deep-CNN models with various configurations. Deep-CNN1 models with Dropout 0.2, Batch 514, and Epoch 2 achieve precisions and F1 scores of 98.88%. As a result, the Deep CNN2 performance for both metrics is reduced to 95.05% when the batch size and epoch are changed to 64 and 15, respectively. Additionally, the proposed LSTM model demonstrates competitive performance compared to other methods evaluated with a precision of 97.06% and an F1 score of 96.60%. Future work will explore more advanced configurations of Deep-CNN models by adjusting batch size and epoch length to improve precision and F1 scores. By leveraging both spatial and temporal characteristics, hybrid models combining CNN and LSTM can be explored for optimizing IoMT RF performance. Incorporating techniques such as data augmentation and regularization can improve model accuracy. Furthermore, CNN and LSTM models could be improved through different activation functions and optimizers. Additionally, large datasets and advanced neural network architectures would demonstrate the robustness and scalability of the models.

Various nodes in the network are shown in Table 4, including their Euclidean distances, RSS vectors, and Si values. Based on their distinct characteristics compared to the rest of the nodes, nodes 6 and 8 are identified as attack nodes. The Si values of nodes 6 and 8 are unusually low, at 325 and 364, which differ significantly from the typical Si range observed in other nodes, which ranges between 650 and 1211.

Table 4. Euclidean distances, RSS vectors, and Si values.

Node	Euclidean Distance	RSS Vector	Si Value
1	194	21.47	1041
2	73	16	869
3	152	10	703
4	233	21.47	652
5	159	21.47	1211
6	97	21.47	364
7	89	21.47	650
8	87	21.47	325

Table 5 shows the reliability analysis results of another scenario in the same experimental dataset. The results of a 5-fold cross-validation on the same experimental dataset, using Random Forest (RF) and Decision Tree algorithms (DT), demonstrate consistent performance. Both models achieved high levels of accuracy, with Random Forest averaging 97.8% (range: 97.5–98.2%) and Decision Tree averaging 97.7% (range: 97.4–98.0%).

To assess the models' ability to discriminate between attack and non-attack classes, we evaluated their ROC-AUC scores. Random Forest outperformed Decision Tree with a score

of 0.92 compared to 0.91, respectively. These results suggest that both models can effectively distinguish between the two classes, with Random Forest exhibiting a slight advantage.

Precision-Recall AUC scores were also calculated to evaluate the models' performance on imbalanced datasets. Random Forest achieved a score of 0.90, indicating a strong balance between precision and recall. Decision Tree followed closely with a score of 0.89, demonstrating comparable performance in this regard.

Table 5. Reliability analysis.

Model	Cross-Validation (5-Fold Accuracy)	ROC-AUC Score	Precision-Recall AUC
Random Forest	Average: 97.8% (Range: 97.5%–98.2%)	0.92	0.90
Decision Tree	Average: 97.7% (Range: 97.4%–98.0%)	0.91	0.89

6. Conclusions and Future Works

In conclusion, DSRM-based IoMT RF spectrum-level threats and mitigation are demonstrated through a hybrid approach. This approach combines localization technique simulation with the deep learning analysis of radio frequency (RF) transmitter nodes and predicts the accuracy of the rogue transmitter. Despite the challenges faced by RSS-based methods, such as multipath propagation, interference, and environmental changes, advanced techniques can mitigate these issues. In addition, adaptive models that learn from changing environments can improve localization accuracy in changing conditions by identifying patterns (IQ Fingerprinting) beyond signal strength. In IoMT environments, RSS can enhance rogue RF transmitter detection reliability by combining it with complementary approaches to DADE, DAL, and signal analysis. RF fingerprinting uses IQ balance datasets derived from Hack-RF device datasets, and RSSI simulation using a Java-based test bed spatial correlation based on received signal strength is proposed—a property of wireless device that is difficult to manipulate. The initial analysis of the IQ data is promising, and proposed research has the potential to be applied in a wide range of applications, such as wireless communication. This research has significantly contributed to improved measures of the IoMT spectrum and further strengthened the security of the connected devices. In addition, the proposed hybrid approach of deep learning and localization can be helpful for other spectrum use cases such as drone technologies, forensic intelligence, and marine solutions. The results can benefit researchers exploring the IoMT spectrum's security further by deploying deception networks and spectrum decoy management. Within the context of the IoMT, we plan to utilize signal intelligence to enhance attack detection frameworks and our attack detection and localization system. The initial attack detection. The framework we developed lays the groundwork for determining rogue transmitters within an IoT environment. We will refine our model's algorithms and deep learning technique so that they can be more accurate, robust, and capable of detecting anomalies in real time. Through several key strategies, this research overcomes the integration challenges and interoperability issues associated with ECC encryption and the use of different programming environments (Python and Java). Python and Java components communicated seamlessly via standard APIs, thereby reducing compatibility concerns. Through a modular design, the ECC encryption module can be developed independently and integrated more easily with other system elements such as front-end stacks (React, Nextjs and Tailwind).

By using data serialization formats (JSON and XML), Python and Java are able to exchange data seamlessly, minimizing data misinterpretation. Developers are guided through best practices through comprehensive documentation, ensuring successful implementation of the framework through interoperability testing to identify and resolve potential integration challenges. We also explore middleware solutions to handle communication between environments, and we adopt CI/CD practices to improve system reliability and functionality by automating testing and continuously validating integration. This research

overcomes the limitations of advanced machine learning techniques despite the fact that they require significant computational resources. By pruning, quantizing, and distilling knowledge, model complexity can be reduced without sacrificing accuracy, making these techniques suitable for environments with limited resources.

Future research will further optimize performance by proposing efficient data processing pipelines, utilizing methods such as data sampling and feature selection to streamline input data and reduce computational load. By combining batch and asynchronous processing approaches, the system can handle multiple data streams more efficiently, improving real-time performance. In addition, a cloud-edge hybrid model will be proposed that ensures flexibility and scalability in resource allocation, making real-time processing feasible even in resource-constrained IoMT environments. We will be integrating advanced data analytics techniques into our attack detection system to enhance its ability to detect attacks more effectively. Another improvement is to develop a predictive analytics system for preventing signal intelligence attacks. This will contribute to proactive crime prevention efforts by preventing attacks on signal intelligence.

Supplementary Materials: The following supporting information can be downloaded at: https://github.com/medikalcoach/RF/ (accessed on 28 December 2023).

Author Contributions: Conceptualization, I.A.J., B.S. and S.A.; methodology, I.A.J. and B.S.; software, I.A.J. and S.A; validation, I.A.J., S.A. and S.T.; formal analysis, I.A.J. and B.S.; resources, S.T.; data curation, I.A.J.; writing—original draft preparation, I.A.J.; writing—review and editing, B.S. and S.A.; supervision, B.S., S.A. and S.T.; project administration, S.T.; funding acquisition, S.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study did not require ethical approval.

Data Availability Statement: The data used to test is available here: https://github.com/medikalcoach/RFIQ/blob/main/IQdataset.csv (accessed on 28 December 2023).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

DADE and DAL Module Experiment and Validation

The wireless nodes are deployed in a network, and received signal strength (RSS) data are collected both during normal operation and when spoofing attacks are suspected. We identified groups of nodes with abnormal behavior by applying the following detection phase techniques to the data, which indicate the presence of an attacker.

A.1. Spoofing Attack Detection Phase

a: Network construction and Euclidean Distance Calculation

- For each pair of nodes (A and B) in the network, calculate the Euclidean distance between the coordinates of node A and node B.
- Store the calculated distance in a matrix or data structure for future use.
- Initialize an empty graph or network structure.
- For each node in the network, assign coordinates or dimensions to the node to represent its position. Connect the node to other nodes to establish communication links.

b: Identify Abnormal Patterns and Detecting Attacker

- Iterate through the stored Euclidean distance values and calculate the average or expected distance between nodes based on network.
- If the calculated distance significantly deviates from the expected value, undertake the following:
- Identify the nodes associated with the abnormal distance as potential attackers.

- Flag these nodes as suspicious or under observation.

c: Report Potential Attackers

- Compile a list of nodes identified as potential attackers.
- Provide this list as output, indicating which nodes are exhibiting abnormal behavior.
- Transmit this information to relevant monitoring or security systems.

A.2. Received Signal Strength Vector

a: Initialize Parameters

- Set up the wireless network environment with source and destination nodes.
- Define the communication range and signal propagation model parameters.

b: File Transfer and Time Calculation

- Select a file to be transferred from the source node to the destination node.
- Initiate the file transfer process.
- Record the start time when the file transfer is initiated.
- Record the end time when the file transfer is completed.
- Calculate the time taken for the file transfer as

$$\text{Transfer\_Time} = \text{End\_Time} - \text{Start\_Time} \tag{A1}$$

c: Calculate Euclidian Distance

- Determine the physical coordinates of the source and destination nodes.
- Based on the coordinates of the source and destination nodes, calculate their Euclidean distance.

d: Received Signal Strength

- Define a path loss model or calibration function to relate the Euclidean distance to RSS.
- Use the calculated Euclidean distance to determine the expected RSS value based on the defined model.
- Optionally, introduce random variations or noise to simulate real-world conditions.

e: Compare Calculated RSS with Measured RSS

- Extract the actual RSS value measured during the file transfer. Compare the calculated RSS value (based on distance and model) with the measured RSS value.
- Calculate the difference between the calculated and measured RSS values as

$$\text{rss\_difference} = \text{measured\_rss} - \text{calculated\_rss} \tag{A2}$$

f: Evaluate and Interpret Results

- Analyze the "rss_difference" to determine the accuracy of the RSS calculation.
- Consider factors such as signal interference, obstacles, and environmental conditions that may contribute to deviations.
- If the difference is within an acceptable threshold, the RSS calculation method is validated.

g: Iterate for Multiple Scenarios

- Repeat the above steps for various source-destination pairs.

- Vary the communication range, file sizes, or network conditions to observe the robustness of the RSS calculation method.

h: Report and Discussion

- Summarize the calculated RSS values, measured RSS values, and corresponding differences.
- Discuss the accuracy and limitations of the RSS calculation method.
- Interpret the results in the context of wireless communication and signal propagation.

A.3. Cluster Analysis

To detect spoofing attackers in physical space using a cluster analysis based on RSS-based spatial correlation, the following algorithmic steps are outlined.

a: Data Collection

- Collect RSS readings from multiple wireless nodes over time.
- Organize the RSS readings into a dataset with each data point representing the RSS values from a specific time interval at a node's location.

b: Spatial Correlation

- Calculate the spatial correlation between pairs of nodes using the collected RSS readings.
- Represent each node's RSS readings as a point in an n-dimensional signal space, where n is the number of time intervals or dimensions.

c: Cluster Formation

- Apply a cluster analysis technique to the dataset in the signal space.
- Group similar RSS patterns together to form clusters.
- Each cluster represents a set of nodes with similar RSS behaviors over time.

d: Medoid Calculation

- For each cluster, calculate the medoid point. The medoid is the data point that has the minimum average dissimilarity to all other points in the same cluster [30].

$$T = D\_m - |M\_i - M\_j| \quad \text{(A3)}$$

$$M\_i \text{ is the medoid of the first cluster.} \quad \text{(A4)}$$

$$M\_j \text{ is the medoid of the first cluster.} \quad \text{(A5)}$$

In our spoofing detection significance tests, we use the distance between the two D_m as the test statistic.

- If the calculated distance between the medoids D_m is greater than a predetermined threshold, Threshold, it suggests a potential presence of a spoofing attack.

$$D\_m > \text{Threshold} \quad \text{(A6)}$$

- If such a scenario occurs, the algorithm may declare that a spoofing attack is present. The threshold value is used to determine the level of dissimilarity in the signal space that triggers the detection. This approach utilizes the distance between medoids as a metric to assess the similarity or dissimilarity of RSS patterns in different clusters, allowing for the identification of significant deviations indicative of spoofing attacks.

e: Distance Calculation

- Calculate the distance between medoids of different clusters.
- The distance metric can be defined based on the characteristics of the signal space and the dissimilarity between medoid points (D_m).

f: Significance Testing
- Define a threshold value that represents a significant distance between medoids.
- Compare the calculated distance between medoids (Dm) to the threshold.
- If Dm exceeds the threshold, it indicates a potential presence of a spoofing attack.

g: Spoofing Attack Detection
- If the calculated Dm is greater than the threshold, declare the presence of a spoofing attack.
- The difference in signal space distances between clusters suggests that the RSS readings are mixed due to the presence of attackers and genuine nodes using the same ID.

h: Result Evaluation and Reporting:
- Analyze the detection results across multiple scenarios and datasets.
- Evaluate the accuracy and false positive/negative rates of the spoofing attack detection based on the chosen distance threshold.
- Discuss the effectiveness of cluster analysis-based methods for detecting spoofing attacks, summarizing, and interpreting the results.

A.4. Attacker Number Detection

The below algorithmic steps outline the process of determining the number of attackers using the System Evolution method based on the twin-cluster model, partition energy, and merging energy calculations. The comparison between partition and merging energies aids in identifying the correct number of clusters (attackers) present in the RSS readings.

a: Attack estimation
- Accurate estimation of the number of attackers is crucial for successful localization.
- The number of attackers is not known beforehand, and it is treated as a multi class detection problem.
- The goal is to determine the number of clusters in the RSS readings, reflecting the number of attackers using the same node identity.

b: System Evolution Method
- Utilize the System Evolution method to analyze cluster structures and estimate the number of clusters (attackers).
- Identify the two closest clusters (clusters “a” and “b”) among the K potential clusters in the dataset.

c: Energy Calculation
- Calculate the partition energy, E_p(K), as the border distance between the twin clusters.
- Calculate the merging energy, E_m(K), as the average distance between elements in the border region of the twin clusters.

d: Number of Attackers Determination
- Compare E_p(n) with E_m(n), where “n” is the current number of clusters under consideration.

$$E\_p(n) > E\_m(n) \tag{A7}$$

- Declare that the number of attackers is “n”.
- Otherwise, declare that the number of attackers is “n+1”.
- The determined number of attackers is used for subsequent steps such as localization.

- This method helps refine the estimation of the number of attackers, enhancing the accuracy of subsequent analysis and actions.

A.5. Detection and Localization Framework:
The below algorithmic steps outline the process of utilizing the integrated detection and localization framework, which combines Bayesian Network localization, spoofing attack detection, and attacker number determination. The integrated approach enhances the accuracy of both detection and localization processes, ultimately contributing to a more secure and effective network environment.

a: Multilateration and Bayesian Graphical Model

- Develop an integrated system capable of detecting spoofing attacks, determining the number of attackers and localizing multiple adversaries.
- Utilize BN (Bayesian Network) localization, which is a multilateration algorithm.
- Encode the signal-to-distance propagation model into the Bayesian Graphical Model for precise localization.

b: Localization Process

- For each node or device, collect RSS readings from multiple reference nodes.
- Measure the Time Differences of Arrival (TDOA) of signals at the reference nodes.
- Utilize the encoded Bayesian Graphical Model to compute the possible location of the node.
- Obtain the sampling distribution of possible X and Y coordinates as the localization result.

c: Detection of Spoofing Attacks

- The localization results provide probable location. coordinates (X and Y) of each node.
- Each set of coordinates corresponds to the possible location of a node in the network.
- Incorporate the calculated localization results with the spoofing attack detection process.
- Compare the localization results with expected behaviors to identify discrepancies that may indicate spoofing.

d: Determining Number of Attackers

- Use the determined localization results to enhance the accuracy of attacker number estimation.
- Utilize the Bayesian Network's output to inform the attacker number determination process.

e: Assessment, Reporting, and Utilization

- Evaluate the integrated framework's performance in terms of accuracy, robustness, and efficiency.
- Analyze the localization results, detection accuracy, and the number of attackers determined.
- Report the integrated results, including detected spoofing attacks, estimated attacker numbers, and the localized positions.
- Discuss the effectiveness of the framework in providing comprehensive security measures and accurate localization capabilities.

References

1. Khan, S.A.; Sundaram, J.; Palendeng, M.; Azam, S.; Shanmugam, B. Simulation of IoT-based smart city of Darwin: Leading cyber attacks and prevention techniques. In Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), New Delhi, India, 6–8 July 2023; pp. 1–9.

2. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
3. Chinaei, M.H.; Gharakheili, H.H.; Sivaraman, V. Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract. *IEEE Internet Things J.* **2021**, *8*, 10117–10130. [CrossRef]
4. Shit, R.C.; Sharma, S.; Puthal, D.; Zomaya, A.Y. Location of Things (LoT): A Review and Taxonomy of Sensors Localization in IoT Infrastructure. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2028–2061. [CrossRef]
5. Denning, E. An Intrusion-Detection Model. *IEEE Trans. Softw. Eng.* **1987**, *13*, 222–232. [CrossRef]
6. Shea, T.; Hoydis, J. An Introduction to Deep Learning for the Physical Layer. *IEEE Trans. Cogn. Commun. Netw.* **2017**, *3*, 563–575. [CrossRef]
7. O'Shea, T.J.; Roy, T.; Clancy, T.C. Over-the-Air Deep Learning Based Radio Signal Classification. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 168–179. [CrossRef]
8. Jalali, M.S.; Kaiser, J.P.; Jarrett, M.; Ghaffarzadegan, N. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [CrossRef]
9. Sackner-Bernstein, J. Design of Hack-Resistant Diabetes Devices and Disclosure of Their Cyber Safety. *J. Diabetes Sci. Technol.* **2016**, *11*, 198–202. [CrossRef]
10. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
11. Wu, R.; Ahn, G.J.; Hu, H. Towards HIPAA-compliant healthcare systems. In Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, Miami, FL, USA, 28–30 January 2012; pp. 593–602.
12. Stewart, R.W.; Crockett, L.; Atkinson, D.; Barlee, K.; Crawford, D.; Chalmers, I.; Mclernon, M.; Sozer, E. A low-cost desktop software defined radio design environment using MATLAB, simulink, and the RTL-SDR. *IEEE Commun. Mag.* **2015**, *53*, 64–71. [CrossRef]
13. Bevly, D.M. Global Positioning System (GPS): A Low-Cost Velocity Sensor for Correcting Inertial Sensor Errors on Ground Vehicles. *J. Dyn. Syst. Meas. Control.* **2004**, *126*, 255–264. [CrossRef]
14. Jagannath, A.; Jagannath, J.; Kumar, P.S.P.V. A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. *Comput. Netw.* **2022**, *219*, 109–455. [CrossRef]
15. Arjoune, Y.; Kaabouch, N. A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions. *Sensors* **2019**, *19*, 126. [CrossRef]
16. Wei, J.; Ji, Y.; Yu, C. Improvement of software defined radio based RSSI localization with bias reduction. *IFAC Proc. Vol.* **2014**, *47*, 7164–7169. [CrossRef]
17. Wei, J.; Yu, C. Improvement of software defined radio based TDOA source localization. In Proceedings of the IECON 2014—40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, USA, 29 October–1 November 2014; pp. 5307–5313.
18. Krishna, K.; Murty, M.N. Genetic K-means algorithm. *IEEE Trans. Syst. Man Cybern. Part B Cybern.* **1999**, *29*, 433–439. [CrossRef] [PubMed]
19. Li, H.; Wang, C.; Ghose, N.; Wang, B. Robust deep-learning-based radio fingerprinting with fine-tuning. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; pp. 395–397.
20. Lee, H.; Kang, T.; Jeong, S.; Seo, J. Evaluation of RF fingerprinting-aided RSS-based target localization for emergency response. In Proceedings of the IEEE Conference on Vehicular Technology (VTC), Helsinki, Finland, 19–22 June 2022; pp. 1–7.
21. Chen, Z.; Peng, L.; Hu, A.; Fu, H. Generative adversarial network-based rogue device identification using differential constellation trace figure. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 72. [CrossRef]
22. Gong, J.; Xu, X.; Lei, Y. Unsupervised Specific Emitter Identification Method Using Radio-Frequency Fingerprint Embedded InfoGAN. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2898–2913. [CrossRef]
23. Kioskli, K.; Fotis, T.; Mouratidis, H. The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–9.
24. Altawy, R.; Youssef, A.M. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access* **2015**, *4*, 959–979. [CrossRef]
25. Lee, J.; Warkentin, M.; Crossler, R.E.; Otondo, R.F. Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *J. Comput. Inf. Syst.* **2016**, *57*, 309–318. [CrossRef]
26. Pritika; Shanmugam, B.; Azam, S. Risk Evaluation and Attack Detection in Heterogeneous IoMT Devices Using Hybrid Fuzzy Logic Analytical Approach. *Sensors* **2024**, *24*, 3223. [CrossRef]
27. Jayaraj, I.A.; Shanmugam, B.; Azam, S.; Samy, G.N. A Systematic Review of Radio Frequency Threats in IoMT. *J. Sens. Actuator Netw.* **2022**, *11*, 62. [CrossRef]
28. Selcuk, A.A. A Guide for Systematic Reviews: PRISMA. *Turk. Arch. Otorhinolaryngol.* **2019**, *57*, 57–58. [CrossRef] [PubMed]
29. Stef, M.P.; Polgar, Z.A. Software Platform for the Comprehensive Testing of Transmission Protocols Developed in GNU Radio. *Information* **2024**, *15*, 62. [CrossRef]

30. Alalyan, F.; Zamzami, N.; Amayri, M.; Bouguila, N. An improved K-medoids algorithm based on binary sequences similarity measures. In Proceedings of the 6th International Conference on Control, Decision and Information Technologies (CoDIT), Paris, France, 23–26 April 2019; pp. 1723–1728.
31. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77. [CrossRef]
32. Flach, P.; Kull, M. Precision-recall-gain curves: PR analysis done right. In Proceedings of the Advances in Neural Information Processing Systems 28: Annual Conference on Neural Information Processing Systems 2015, Montreal, QC, Canada, 7–12 December 2015.
33. Sayakkara, A.P.; Le-Khac, N.-A. Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets. *IEEE Access* **2021**, *9*, 113585–113598. [CrossRef]
34. Zhang, J.; Woods, R.; Sandell, M.; Valkama, M.; Marshall, A.; Cavallaro, J. Radio Frequency Fingerprint Identification for Narrowband Systems, Modelling and Classification. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3974–3987. [CrossRef]
35. Acharya, U.R.; Oh, S.L.; Hagiwara, Y.; Tan, J.H.; Adam, M.; Gertych, A.; San Tan, R. A deep convolutional neural network model to classify heartbeats. *Comput. Biol. Med.* **2017**, *89*, 389–396. [CrossRef]
36. Guazzo, M. Retrieval performance and information theory. *Inf. Process. Manag.* **1977**, *13*, 155–165. [CrossRef]
37. Roy, D.; Mukherjee, T.; Chatterjee, M.; Pasiliao, E. Detection of rogue RF transmitters using generative adversarial nets. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakech, Morocco, 15–18 April 2019; pp. 1–7.
38. Dokmanic, I.; Parhizkar, R.; Ranieri, J.; Vetterli, M. Euclidean distance matrices: Essential theory, algorithms, and applications. *IEEE Signal Process. Mag.* **2015**, *32*, 12–30. [CrossRef]