Security and Privacy Considerations in Machine Learning-Enhanced Cognitive Radio Path Loss Models

1. Introduction: Cognitive Radio, Machine Learning in Path Loss Modeling, and the Imperative of Security and Privacy

Cognitive radio (CR) technology has emerged as a promising paradigm to address the growing demand for radio spectrum by enabling wireless devices to dynamically adapt their transmission parameters to the surrounding radio environment.[1] This intelligent approach allows for efficient spectrum utilization by sensing available channels and configuring the radio accordingly, a process known as dynamic spectrum management.[1] As the complexity and density of wireless networks increase, the integration of machine learning (ML) into CR systems offers significant potential for enhancing various functionalities, particularly in the realm of path loss modeling.[2] Accurate prediction of path loss, which describes the attenuation of a radio signal as it propagates through space, is crucial for efficient network planning and operation. Machine learning algorithms can learn intricate patterns from data, potentially leading to more accurate and adaptable path loss models compared to traditional analytical or empirical methods.[2]

However, the incorporation of machine learning into cognitive radio networks also introduces new challenges, particularly concerning security and privacy.[6] The intelligent and adaptive nature of these systems, coupled with the data-driven characteristics of machine learning, creates novel attack vectors and privacy risks that must be thoroughly understood and addressed. Ensuring the reliable and trustworthy operation of machine learning-enhanced cognitive radio networks necessitates a comprehensive investigation into these security and privacy aspects, especially during the critical training phase of the machine learning models. This report aims to explore the security and privacy risks associated with the training and deployment of machine learning-enhanced path loss models in cognitive radio systems, to investigate existing and proposed mitigation strategies to address these risks, and to provide practical guidance on how these findings can be effectively incorporated into a dissertation focusing on this topic.

2. Fundamentals of Cognitive Radio and Machine Learning for Path Loss Prediction

- **Overview of Cognitive Radio Technology:**

Cognitive radio represents a significant evolution in wireless communication, moving towards systems that are aware of their operational environment and can adapt their

behavior accordingly.[1] At its core, CR technology is about enabling radios to make intelligent decisions regarding spectrum use. This intelligence is achieved through key functionalities such as spectrum sensing, which involves detecting the presence of other signals in the radio environment to identify unused frequency bands.[1] For instance, energy detection is a common spectrum sensing method that measures the received signal power to determine if a channel is occupied.[1] Spectrum management is another crucial function, encompassing the decisions a CR makes about which frequency band to utilize and with what transmission parameters to meet user needs while minimizing interference.[1] The ultimate goal of these functionalities is to enable dynamic spectrum access (DSA), allowing secondary users (CRs) to opportunistically utilize spectrum that is not currently being used by primary, licensed users.[1] This dynamic access addresses the growing problem of spectrum scarcity by allowing more efficient use of available radio frequencies.[1] The foundation for the flexibility of cognitive radio lies in software-defined radio (SDR) technology, which provides the reconfigurable hardware and software platform necessary to implement these dynamic capabilities.[1] The ability of a CR to learn and adapt makes it a prime candidate for integration with machine learning techniques, which can further enhance its intelligence and decision-making processes in complex and dynamic radio environments. However, this very flexibility also introduces potential security vulnerabilities that must be carefully considered.[6]

- **Application of Machine Learning in Path Loss Modeling: Advantages and Common Techniques:**

Accurate prediction of path loss is essential for the effective planning and deployment of wireless networks, including those employing cognitive radio technology.[2] Traditional methods for path loss prediction often rely on empirical models derived from measurements or deterministic models based on physical principles.[2] However, these models can be limited in their accuracy and applicability, especially in complex urban or indoor environments where signal propagation is affected by numerous factors.[2] Machine learning offers a powerful alternative by enabling the development of path loss models that can learn intricate relationships from data, leading to increased accuracy and better adaptability to diverse environments.[2] Various machine learning techniques are employed for this purpose. Artificial Neural Networks (ANNs) and Deep Learning (DL) models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown significant promise in capturing the non-linear relationships between input features (like distance, frequency, antenna height, and environmental data) and path loss.[2] Support Vector Machines (SVMs) are another popular choice for regression tasks like path loss prediction, known for their effectiveness in high-dimensional spaces.[2] Regression algorithms such as Linear

Regression and Random Forests are also utilized for their simplicity and ability to model the dependence of path loss on various parameters.[2] Furthermore, ensemble methods, which combine the predictions of multiple models, can often achieve higher accuracy and robustness.[2] The increasing interest in distributed learning has also led to the application of federated learning for path loss modeling in cognitive radio networks, allowing for collaborative training on decentralized data while preserving privacy.[22] The choice of the specific ML technique depends on the characteristics of the data available and the requirements of the CR application.

3. Security Risks During the Training Phase

- **Data Poisoning Attacks: Impact on Model Accuracy and Reliability:**

A significant security risk during the training phase of machine learning models in cognitive radio networks is data poisoning. This type of attack involves the intentional injection of malicious or manipulated data into the training dataset, with the goal of corrupting the learning process and causing the resulting path loss model to make inaccurate predictions or exhibit undesirable behavior.[59] In the context of path loss modeling for cognitive radios, such attacks could have severe consequences, leading to inaccurate estimations of signal propagation, which in turn can negatively impact spectrum sensing and allocation decisions. Various forms of data poisoning attacks exist. In federated learning scenarios, Byzantine attacks can occur where compromised cognitive radio nodes send arbitrary or incorrect updates to the central server, disrupting the training of the global path loss model.[52] Label flipping attacks involve altering the labels associated with training data; for instance, mislabeling path loss measurements taken under specific environmental conditions could skew the model's understanding of these conditions' impact on signal attenuation.[71] Feature manipulation attacks involve subtly modifying the input features, such as the reported distance or terrain characteristics, which can be difficult to detect but can still affect the learned model.[71] Backdoor attacks involve injecting specific data points designed to introduce a hidden trigger into the model, causing it to behave maliciously when this trigger is present in the input, even if the input otherwise appears normal.[73] The success of data poisoning attacks can significantly degrade the accuracy and reliability of path loss prediction models, potentially leading secondary users to make incorrect assumptions about spectrum availability, causing interference to primary users, or failing to utilize available spectrum efficiently.[71] Detecting these attacks can be particularly challenging, especially in distributed learning environments like federated learning, where the training data is spread across numerous devices with limited central oversight.[57]

- **Adversarial Training Vulnerabilities: Exploiting the Training Process:**

Adversarial training is a defense mechanism aimed at improving the robustness of machine learning models against adversarial attacks by training them on both clean data and intentionally perturbed adversarial examples.[77] However, the adversarial training process itself can be vulnerable to exploitation. Attackers might craft specific adversarial examples during training to introduce subtle weaknesses or backdoors into the path loss model that can be exploited later during deployment.[70] For instance, an adversary could try to create adversarial examples that, while appearing normal, cause the model to consistently underestimate path loss under certain conditions that the attacker can then exploit to transmit at higher power levels without being detected as interfering. Furthermore, adversarial examples crafted for one model can sometimes be effective against other models, even those that have undergone adversarial training, a phenomenon known as transferability.[106] This means that a path loss model in a cognitive radio network might be vulnerable to attacks developed for a different, seemingly unrelated system. Another consideration is the inherent trade-off in adversarial training, where increasing the model's resilience to adversarial examples can sometimes lead to a reduction in its accuracy on clean, unperturbed data.[77] Therefore, a careful balance must be struck to ensure that the path loss model remains accurate and reliable for its intended use while also being robust against malicious manipulation.

- **Other Potential Security Threats During Model Training:**

Beyond data poisoning and vulnerabilities in adversarial training, other security threats can arise during the training phase of machine learning models for cognitive radio path loss prediction. One such threat is model theft or extraction, where an attacker attempts to steal the trained model.[85] By querying the model with various inputs and analyzing the outputs, an adversary might be able to approximate the model's architecture and parameters, gaining access to potentially sensitive information about the cognitive radio network's characteristics or the behavior of its users. Backdoor attacks represent another significant risk, where attackers inject specific data into the training set that introduces a hidden trigger. When this trigger is present in the input at deployment time, it can cause the model to behave in a predetermined malicious way, such as providing incorrect path loss predictions under specific, attacker-controlled conditions.[85] Finally, the integrity of the training infrastructure itself could be compromised, allowing attackers to directly manipulate the training data, the learning algorithm, or the model parameters, leading to a severely flawed or biased path loss model.

4. Privacy Risks During the Training Phase

- **Information Leakage from Training Datasets:**

The training datasets used for machine learning-based path loss models in cognitive radio networks often contain sensitive information that could be unintentionally leaked during the training process.[10] This data can include the precise geographical locations of primary and secondary users, detailed characteristics of the terrain and environment affecting signal propagation, and specific communication parameters like operating frequencies and transmission power levels. If an attacker were to gain access to this training data, they could potentially infer a significant amount of private information about the network's deployment, the activities of its users, and even the operational capabilities of the systems.[11] In scenarios where machine learning models are trained on distributed data in cognitive radio networks, such as through federated learning, preserving the privacy of this information becomes even more challenging.[53] Even though federated learning aims to keep raw data localized on individual devices, the shared model updates could still potentially leak sensitive information about the underlying training data if not properly protected.[53] Therefore, it is crucial to implement robust data anonymization and protection techniques to mitigate these risks and ensure the privacy of users and the security of the network.[10]

- **Membership Inference Attacks on Path Loss Models:**

Another privacy risk during the training phase is the potential for membership inference attacks on the trained path loss models.[111] In this type of attack, an adversary tries to determine if a specific data point, such as a particular path loss measurement taken at a certain location and time, was part of the training dataset used to build the model. A successful membership inference attack on a path loss model could reveal sensitive information about the data collection process or the specific locations and times at which measurements were taken, potentially compromising the privacy of users or revealing details about the network environment.[111] For instance, if an attacker suspects that path loss data was collected from a specific primary user's transmitter location, they could try to infer whether a measurement corresponding to that location was used to train the model. Confirming membership could reveal the primary user's operational area or activity patterns. Defending against membership inference attacks is challenging because machine learning models often inherently memorize some aspects of their training data, making it difficult to completely prevent the leakage of this type of information.[111]

- **Other Privacy Considerations in the Training Pipeline:**

Beyond information leakage from the training data itself and membership inference

attacks, other privacy considerations need to be addressed during the training of machine learning models for cognitive radio path loss prediction. One important aspect is the use of differential privacy, a technique that adds a carefully calibrated amount of random noise to the training data or the model updates to limit the amount of information that can be learned about any individual data point in the training set.[54] While differential privacy can provide a quantifiable privacy guarantee, it often involves a trade-off with the accuracy of the resulting model. Another consideration is the privacy implications of hyperparameter tuning and model selection. The process of finding the optimal hyperparameters and model architecture might inadvertently reveal information about the characteristics of the training data. Therefore, it is important to consider privacy-preserving techniques for these aspects of the training pipeline as well. Model inversion attacks, where an attacker tries to reconstruct the training data from the trained model itself, also represent a potential privacy risk.[109]

5. Security Threats and Vulnerabilities in Deployed Models

- **Adversarial Attacks on Trained Path Loss Prediction Models:**

Once a machine learning model for path loss prediction is trained and deployed in a cognitive radio network, it becomes susceptible to adversarial attacks.[9] These attacks involve carefully crafting adversarial inputs, which are often imperceptibly perturbed versions of legitimate inputs, designed to cause the model to produce incorrect outputs. In the context of path loss prediction, an attacker might slightly modify the reported distance between a transmitter and receiver or the environmental parameters to cause the model to predict a significantly different path loss value than what would actually occur.[77] The impact of such attacks on cognitive radio networks can be substantial. For instance, misleading path loss predictions could lead secondary users to make incorrect decisions about spectrum access, potentially causing harmful interference to primary users if they transmit at higher power levels than necessary, or underutilizing available spectrum if they believe the path loss is higher than it actually is.[70] Evasion attacks, which occur at the inference stage, are a common type of adversarial attack where the goal is to "fool" the deployed model into making a wrong prediction.[70]

- **Spectrum Sensing Deception Enabled by Model Manipulation:**

Manipulating the deployed path loss model can also enable more sophisticated spectrum sensing deception attacks in cognitive radio networks.[8] For example, by carefully crafting inputs to the path loss model, an attacker might be able to create scenarios where the model predicts a very low path loss in a frequency band that is actually occupied by a primary user, thus deceiving secondary users into believing the

spectrum is free. This is closely related to primary user emulation (PUE) attacks, where a malicious secondary user tries to mimic the signal characteristics of a primary user to gain unauthorized access to the licensed spectrum.[8] A compromised path loss model could provide valuable information to the attacker on how to make their emulated signal more convincing by predicting the expected signal strength and propagation characteristics of a legitimate primary user at a given location. Similarly, in spectrum sensing data falsification (SSDF) attacks, where malicious secondary users send false sensing reports to a fusion center, a manipulated path loss model could help the attackers generate falsified reports that are consistent with the expected signal propagation patterns, making their deception harder to detect.[8]

- **Other Security Concerns in Operational Cognitive Radio Networks:**

Beyond adversarial attacks and spectrum sensing deception, other security concerns in operational cognitive radio networks can be exacerbated by vulnerabilities in deployed machine learning models. Jamming attacks, where an adversary intentionally transmits signals to interfere with legitimate communication, might become more effective if the attacker can leverage a compromised path loss model to identify the optimal times and frequencies to jam, or to predict how secondary users will react to the jamming.[9] Eavesdropping, where an unauthorized party tries to intercept and decode communication signals, could also be facilitated if an attacker can use a manipulated path loss model to identify the best locations for placing eavesdropping devices or to analyze intercepted signals more effectively.[8] Denial-of-service (DoS) attacks, aimed at disrupting the availability of network resources, could also potentially exploit vulnerabilities in the deployed machine learning models to cause network instability or prevent legitimate users from accessing the spectrum.[9]

6. Privacy Concerns Related to Training Data

- **Sensitivity of Location and Communication Parameters:**

The training data used to develop machine learning-based path loss models in cognitive radio networks often contains highly sensitive information about the users and the network environment.[11] This includes the geographical locations of both primary (licensed) and secondary (unlicensed) users, detailed characteristics of the terrain and physical environment that influence radio wave propagation, and specific communication parameters such as the operating frequencies, bandwidths, and transmission power levels employed by different users.[11] This seemingly technical data can be directly linked to individual users or specific organizations and can reveal a significant amount of private information about their activities, movements, and

communication patterns.[11] For instance, the location data of a user's device, even if anonymized, can potentially be used to track their movements and infer their daily routines. Information about the frequency bands they use or their transmission power levels might reveal the type of services they are accessing or their network usage habits. The sensitivity of this data necessitates careful consideration of privacy implications throughout the lifecycle of the machine learning model, from data collection to training and deployment.

- **Risks of Data Re-identification and Attribute Inference:**

Even if direct identifiers such as user IDs or specific device addresses are removed from the training data used for path loss models, there remains a significant risk of re-identification and attribute inference.[112] Sophisticated adversaries can employ various techniques, such as linkage attacks, to combine the anonymized training data with other publicly available information or previously compromised datasets to potentially re-identify individuals or specific locations.[112] Furthermore, even without direct re-identification, an attacker might be able to infer sensitive attributes about users or the network environment by analyzing the patterns and correlations within the path loss data itself.[112] For example, unique patterns in signal attenuation observed at certain times of day or in specific geographical areas might allow an attacker to infer user activity patterns, the type of devices being used, or the density of users in a particular region, even if the explicit identity of the users remains unknown. These risks highlight the limitations of traditional anonymization techniques and underscore the need for more advanced privacy-preserving approaches when dealing with the sensitive data used for training machine learning models in cognitive radio networks.

- **Compliance with Privacy Regulations and Standards:**

The collection, processing, and storage of data used for training machine learning models in cognitive radio networks, particularly if this data includes any information that could be considered personally identifiable (such as location data or communication patterns), must adhere to relevant privacy regulations and standards.[117] Regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States impose strict requirements on organizations regarding the handling of personal data, including the need for explicit consent, data minimization, and the implementation of appropriate security measures to protect against unauthorized access and disclosure.[117] Failure to comply with these regulations can result in significant legal and financial penalties, as well as damage to the reputation and trustworthiness of the cognitive radio network operator. Therefore, it is crucial to carefully consider the privacy implications of data collection and usage throughout the development and

deployment of machine learning-enhanced cognitive radio systems and to implement appropriate privacy-preserving techniques to ensure compliance with all applicable regulations and standards.

7. Mitigation Strategies and Defense Mechanisms

- **Defenses Against Data Poisoning Attacks in Federated and Centralized Learning:**

To mitigate the threat of data poisoning attacks in machine learning-enhanced cognitive radio networks, various defense mechanisms can be employed in both centralized and federated learning settings.[4] In federated learning, robust aggregation techniques, such as using the geometric median to aggregate model updates from different clients, can help to reduce the impact of malicious or outlier updates sent by poisoned nodes.[64] Data sanitization methods, including outlier detection techniques based on statistical methods or machine learning algorithms, can be used to identify and remove potentially poisoned data points from the training set in both centralized and federated scenarios.[4] Implementing strict data validation and filtering mechanisms on the incoming training data can also help to detect and block some forms of poisoned samples.[83] Monitoring the behavior of the machine learning model during training for any unusual patterns or anomalies can provide an early indication of a potential data poisoning attack.[52] In distributed learning, Byzantine fault tolerance techniques can be employed to ensure the reliability of the learning process even in the presence of malicious participants sending faulty updates.[52] Furthermore, researchers are exploring attack-agnostic defense strategies that aim to be effective against a wide range of poisoning attacks without requiring specific knowledge of the attack method [93], as well as certified defenses that offer provable guarantees on the model's robustness.[133]

- **Techniques for Robust Adversarial Training in Wireless Communication Systems:**

To enhance the resilience of path loss models and other machine learning components in cognitive radio networks against adversarial attacks, various robust adversarial training techniques can be employed.[12] One approach is to train the model using a diverse set of adversarial examples generated by different attack methods, which helps the model learn to generalize its defenses against a wider range of potential manipulations.[106] Defense mechanisms that exploit the sensitivity of deep learning models to errors in the training data can also be effective in improving robustness.[70] Input transformation techniques, such as randomly resizing or rotating the input data during training and inference, can help to disrupt the patterns that

adversarial attacks rely on.[106] Knowledge distillation, where a more robust "teacher" model is used to train a less robust "student" model, can also enhance the student's resilience.[105] Adversarial pre-training followed by fine-tuning on clean data is another strategy to learn more robust feature representations.[75] Finally, randomized smoothing techniques, which involve adding random noise to the input at test time and aggregating the predictions, can provide a probabilistic guarantee of robustness against certain types of adversarial attacks.[133]

- **Privacy-Preserving Machine Learning Approaches for Path Loss Modeling:**

To train accurate path loss models in cognitive radio networks while protecting the privacy of the sensitive training data, several privacy-preserving machine learning approaches can be utilized.[53] Federated learning (FL) with secure aggregation is a promising technique that allows multiple cognitive radio nodes to collaboratively train a shared path loss model without exchanging their raw measurement data.[41] Differential privacy (DP) can be employed to add a carefully calibrated amount of noise to the training data or the model updates to limit the information leakage about individual data points.[54] Homomorphic encryption (HE) is another advanced technique that allows computations to be performed on encrypted data, which could potentially be used to encrypt model updates in federated learning.[53] Various privacy-preserving data aggregation techniques beyond secure aggregation in FL also exist, such as secure multi-party computation (SMPC) protocols, which enable multiple parties to compute an aggregate result without revealing their individual inputs.[57]

- **Security Measures for Protecting Deployed Machine Learning Models in Cognitive Radios:**

Once machine learning-based path loss models are deployed in cognitive radio devices or network infrastructure, several security measures can be implemented to protect them from attacks.[8] Input validation and sanitization techniques can be used to check the inputs fed into the model and filter out any potentially malicious or adversarial data.[83] Anomaly detection mechanisms can monitor the model's predictions and behavior for any unusual patterns that might indicate an ongoing attack or a compromise of the model.[83] Ensuring the secure storage and deployment of the models is also crucial to prevent unauthorized access or tampering. This might involve using encryption and access control mechanisms. Regular updates and patching of the deployed models are necessary to address any newly discovered vulnerabilities and to incorporate improvements in security based on the evolving threat landscape. Continuous monitoring of the cognitive radio network for suspicious activities, such as unexpected spectrum usage patterns or interference, can also help

in detecting and responding to attacks targeting the machine learning components.

8. Implementation and Evaluation of Mitigation Strategies in Cognitive Radio Scenarios

- **Practical Considerations for Deploying Security and Privacy Enhancements:**

Deploying security and privacy enhancements for machine learning-enhanced cognitive radio networks presents several practical considerations.[12] Cognitive radio devices are often resource-constrained in terms of computational power, memory, and energy. Therefore, the mitigation strategies implemented must be lightweight and efficient to avoid significantly impacting the device's performance or battery life.[137] The dynamic nature of the radio environment in which cognitive radios operate also poses a challenge. Security and privacy mechanisms need to be adaptable and able to function effectively under varying channel conditions and interference levels.[12] Furthermore, many cognitive radio applications require low-latency operation, which means that the added overhead of security and privacy measures should not introduce unacceptable delays in the network's response time. This often necessitates a careful trade-off between the level of security and privacy achieved and the overall performance of the cognitive radio system.

- **Performance Evaluation Metrics for Security and Privacy:**

Evaluating the effectiveness of the proposed mitigation strategies requires the use of appropriate performance metrics. For security, relevant metrics include the detection rate of data poisoning attacks, which measures the percentage of malicious data that is correctly identified.[52] The false alarm rate is also important, indicating how often legitimate data or behavior is incorrectly flagged as an attack.[47] For evaluating the robustness against adversarial attacks, the attack success rate, which is the percentage of attacks that manage to fool the model despite the defenses, is a key metric.[80] For privacy, in the context of differential privacy, the privacy budget (defined by parameters epsilon and delta) quantifies the level of privacy protection.[54] The accuracy of membership inference attacks, which measures how well an adversary can determine if a data point was in the training set, can also be used to assess privacy.[111] Information leakage metrics, such as mutual information, can provide a measure of the amount of sensitive information revealed by the model or the training process.[119]

- **Examples of Implementation Frameworks and Testbeds:**

Researchers often utilize various simulation tools and frameworks to implement and evaluate security and privacy mitigation strategies for cognitive radio networks.

Network simulators like NS-3 and OMNeT++ provide environments for modeling wireless communication systems and can be extended to incorporate machine learning functionalities and security attack scenarios.[52] For privacy-preserving machine learning techniques, frameworks like TensorFlow Privacy and PyTorch Privacy offer implementations of differential privacy and secure aggregation protocols.[93] Software-defined radios (SDRs) provide a valuable platform for building practical testbeds to experiment with cognitive radio concepts and to evaluate the effectiveness of security and privacy measures in real-world scenarios.[47]

9. Incorporating Security and Privacy Research into Your Dissertation

- **Key Findings and Aspects to Highlight in Relevant Chapters:**

The findings from your research on the security and privacy aspects of using machine learning in cognitive radio path loss models should be integrated throughout your dissertation. In the introduction, it is important to highlight the significance of these concerns and how your research aims to address them. The literature review chapter should provide a comprehensive overview of existing work on security and privacy in cognitive radio networks, machine learning security and privacy, and specifically in the context of wireless communication and path loss modeling. You should clearly identify the gaps in the current knowledge that your dissertation will contribute to. The methodology chapter should detail the specific machine learning techniques you are using for path loss modeling and, crucially, how you are incorporating security and privacy considerations into your approach. This might include describing the defense mechanisms you are implementing against data poisoning or adversarial attacks, the privacy-preserving techniques you are employing, and the evaluation metrics you will use to assess both the performance of your path loss model and the effectiveness of your security and privacy measures. The results chapter will then present the outcomes of your experiments and analysis, quantifying the security risks you investigated and the effectiveness of your mitigation strategies. The discussion chapter should analyze and interpret your findings, discuss their implications for the security and privacy of machine learning-enhanced cognitive radio networks, compare your results with existing research, and highlight the novel contributions of your work. Finally, the conclusion chapter should summarize the key findings related to security and privacy and reiterate their significance in the context of your overall dissertation.

- **Suggested Structure for Dissertation Chapters on Security and Privacy in Cognitive Radio with ML:**

A potential structure for dissertation chapters focusing on security and privacy in the

context of your machine learning-enhanced cognitive radio path loss model could be as follows:

1. **Introduction:** Introduce the chapter's specific focus on security and privacy within your research. Clearly state the research questions or objectives related to these aspects.
2. **Literature Review:** Provide a focused review of existing research on security and privacy challenges in cognitive radio networks, machine learning security and privacy, and specifically in the context of wireless communication and path loss modeling. Highlight the gaps in the literature that your research aims to address.
3. **Methodology:** Detail the machine learning techniques used for path loss modeling. Explain how you are incorporating security and privacy considerations into your training process (e.g., defenses against data poisoning, adversarial training, privacy-preserving techniques). Describe the evaluation metrics you will use for both the performance of your path loss model and the effectiveness of your security and privacy measures. Specify the simulation environment or testbed you are using.
4. **Results:** Present the results of your experiments, showing the performance of your path loss model under normal conditions and under various security and privacy attacks. Quantify the effectiveness of the mitigation strategies you have implemented using the chosen evaluation metrics.
5. **Discussion:** Analyze and interpret your findings. Discuss the implications of your results for the security and privacy of ML-enhanced cognitive radio networks. Compare your findings with existing research and highlight the novel contributions of your work. Address any limitations of your study and suggest directions for future research.
6. **Conclusion:** Summarize the key findings of the chapter and reiterate their significance in the context of your overall dissertation.

- **Examples of Academic Report Structures for Dissertation Chapters in Technical Domains:**

The following table provides a general structure that is commonly used for dissertation chapters in technical domains, which you can adapt for your chapters focusing on security and privacy in machine learning-enhanced cognitive radio path loss models [109]:

Section	Description	Focus in Your Dissertation
Introduction	Briefly introduces the topic of the chapter and its relevance	Introduce the specific security and privacy challenges you

	to the overall dissertation. States the chapter's objectives and scope.	are addressing in this chapter within the context of your ML-enhanced cognitive radio path loss model. State your research questions or objectives related to these aspects.
Background/Related Work	Provides necessary background information and reviews relevant literature, highlighting existing knowledge and gaps that the chapter will address.	Review existing research on security and privacy risks in cognitive radio networks that utilize machine learning, specifically in the domain of path loss modeling. Highlight the gaps in the current research that your work aims to fill.
Methodology	Details the methods, techniques, and experimental setup used in the research presented in the chapter. Explains the rationale behind the chosen approach.	Detail the specific machine learning techniques you are using for path loss prediction. Critically explain how you are incorporating security and privacy considerations into your methodology, such as the defenses against data poisoning you are implementing, the adversarial training techniques you are employing, or the privacy-preserving machine learning approaches you are investigating. Describe the evaluation metrics you will use to assess both the performance of your path loss model and the effectiveness of your security and privacy measures. Clearly specify the simulation environment or experimental testbed you are using.
Results	Presents the findings of the research, typically using	Present the outcomes of your experiments in a clear and

	figures, tables, and statistical analysis. Focuses on objective reporting of the outcomes.	organized manner. Show the performance of your path loss model under normal operating conditions. Then, present the results of your evaluations of the security and privacy aspects, such as the model's resilience to data poisoning and adversarial attacks, and the level of privacy protection achieved by your chosen techniques, using the metrics you defined in the methodology.
Discussion	Interprets the results, discusses their significance in the context of the research questions and existing literature. Addresses limitations and suggests future directions.	Analyze and interpret the results you have presented. Discuss the implications of your findings for the security and privacy of machine learning-enhanced cognitive radio networks used for path loss prediction. Compare your results with the existing literature you reviewed and highlight the novel contributions of your research in addressing the identified gaps. Acknowledge any limitations of your study and suggest potential directions for future research in this area.
Conclusion	Summarizes the main findings of the chapter and their contribution to the overall dissertation argument. May also briefly preview the next chapter.	Summarize the key findings of this part of your dissertation, emphasizing their significance in the broader context of secure and private wireless communications. Briefly reiterate how your research contributes to the overall goals of your dissertation.

10. Conclusion: Summary of Key Risks, Mitigation Strategies, and

Recommendations for Dissertation Integration

In conclusion, the integration of machine learning into cognitive radio networks for path loss modeling presents significant opportunities for enhanced spectrum utilization and network performance. However, this integration also introduces critical security and privacy challenges that must be addressed to ensure the reliable and trustworthy operation of these systems. During the training phase, machine learning models are vulnerable to data poisoning attacks that can severely impact their accuracy and reliability, as well as to exploitation through adversarial training. Privacy risks during training include the potential leakage of sensitive information from the training datasets and the possibility of membership inference attacks. Deployed models face threats from adversarial attacks that can manipulate their predictions and from spectrum sensing deception enabled by model manipulation. The training data itself often contains sensitive location and communication parameters, raising concerns about data re-identification and attribute inference, and necessitating compliance with privacy regulations. To mitigate these risks, various strategies can be employed, including robust aggregation techniques, data sanitization, adversarial training, and privacy-preserving machine learning approaches like federated learning and differential privacy. The practical implementation of these strategies in resource-constrained cognitive radio scenarios requires careful consideration of computational overhead and performance trade-offs. Evaluating the effectiveness of these measures necessitates the use of appropriate security and privacy metrics. The findings from this research should be carefully integrated into the dissertation, with dedicated chapters or sections focusing on the identified risks, the proposed and evaluated mitigation strategies, and a thorough discussion of the results and their implications for the field of cognitive radio and machine learning security and privacy. By addressing these aspects comprehensively, the dissertation can contribute valuable insights to the development of secure and privacy-respecting machine learning-enhanced cognitive radio networks.

Works cited

1. Cognitive radio - Wikipedia, accessed on April 9, 2025, https://en.wikipedia.org/wiki/Cognitive_radio
2. A Machine Learning Approach for Path Loss Prediction Using Combination of Regression and Classification Models - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/24/17/5855
3. A Machine Learning Approach for Path Loss Prediction Using Combination of Regression and Classification Models - PubMed, accessed on April 9, 2025, https://pubmed.ncbi.nlm.nih.gov/39275766/
4. Accurate Path Loss Prediction Using a Neural Network Ensemble Method - PMC,

accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10781234/
5. Procedure of machine-learning-based path loss prediction. - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/figure/Procedure-of-machine-learning-based-path-loss-prediction_fig2_332976325
6. Cognitive Radios: Pioneering Intelligent Communication Systems - ArcticToday, accessed on April 9, 2025, https://www.arctictoday.com/%F0%9F%87%AB%F0%9F%87%AE-cognitive-radios-pioneering-intelligent-communication-systems/
7. Essentials of Cognitive Radio - Cambridge University Press & Assessment, accessed on April 9, 2025, https://www.cambridge.org/core/books/essentials-of-cognitive-radio/F3D835ED585A643A3D654AF594345AE7
8. Security Threat Analysis in 5G Cognitive Radio Networks: A Deep Learning Ensemble Approach - IIETA, accessed on April 9, 2025, https://iieta.org/download/file/fid/157285
9. A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/260686451_A_Survey_of_Security_Challenges_in_Cognitive_Radio_Networks_Solutions_and_Future_Research_Directions
10. Secure channel estimation model for cognitive radio network physical layer security using two-level shared key authentication, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11743765/
11. AI/ML in 5G Spectrum Sharing Security - IEEE Communications Society Cognitive Networks Technical Committee, accessed on April 9, 2025, https://cn.committees.comsoc.org/files/2021/03/cogsec_seminar_jan21.pdf
12. Deep Learning Frameworks for Cognitive Radio Networks: Review and Open Research Challenges - arXiv, accessed on April 9, 2025, https://arxiv.org/html/2410.23949v1
13. Some Fundamental Limits on Cognitive Radio - People @EECS, accessed on April 9, 2025, https://people.eecs.berkeley.edu/~sahai/Papers/cognitive_radio_preliminary.pdf
14. Spectrum Sensing for Cognitive Radio: Fundamentals and Applications - - Routledge, accessed on April 9, 2025, https://www.routledge.com/Spectrum-Sensing-for-Cognitive-Radio-Fundamentals-and-Applications/Captain-Joshi/p/book/9781032126050
15. Some Fundamental Limitations for Cognitive Radio - People @EECS, accessed on April 9, 2025, https://people.eecs.berkeley.edu/~sahai/Presentations/cognitive_presentation.pdf
16. Principles of Cognitive Radio - Assets - Cambridge University Press, accessed on April 9, 2025, https://assets.cambridge.org/97811070/28753/frontmatter/9781107028753_frontmatter.pdf
17. Fundamentals of Cognitive Radio | Wiley, accessed on April 9, 2025,

https://www.wiley.com/en-us/Fundamentals+of+Cognitive+Radio-p-x000601705
18. Fundamentals of Cognitive Radio (Adaptive and Cognitive Dynamic ..., accessed on April 9, 2025, https://www.amazon.com/Fundamentals-Cognitive-Adaptive-Dynamic-Systems/dp/1118302966
19. Machine Learning-Based Path Loss Modeling with Simplified Features - arXiv, accessed on April 9, 2025, https://arxiv.org/html/2405.10006v1
20. Path Loss Prediction Based on Machine Learning Techniques: Principal Component Analysis, Artificial Neural Network, and Gaussian Process - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/20/7/1927
21. Methods for Path loss Prediction - DiVA portal, accessed on April 9, 2025, https://www.diva-portal.org/smash/get/diva2:273839/FULLTEXT01.pdf
22. Path Loss Prediction Based on Machine Learning Techniques: Principal Component Analysis, Artificial Neural Network, and Gaussian Process - PubMed Central, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC7181246/
23. Propagation Issues for Cognitive Radio - WiDeS - USC, accessed on April 9, 2025, https://wides.usc.edu/Updated_pdf/molisch2009propagation.pdf
24. Path Loss Prediction in Tropical Regions using Machine Learning Techniques: A Case Study - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2079-9292/11/17/2711
25. Comparative Analysis of Major Machine-Learning-Based Path Loss Models for Enclosed Indoor Channels - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/22/13/4967
26. [1410.3145] Machine Learning Techniques in Cognitive Radio Networks - ar5iv - arXiv, accessed on April 9, 2025, https://ar5iv.labs.arxiv.org/html/1410.3145
27. Advancements in Machine Learning Techniques for Optimizing Cognitive Radio Networks: A Comprehensive Review - Semantic Scholar, accessed on April 9, 2025, https://pdfs.semanticscholar.org/331a/7963984e6eeafdc7ac6549b5019305ff5b27.pdf
28. Applications of Machine Learning to Cognitive Radio Networks | Request PDF, accessed on April 9, 2025, https://www.researchgate.net/publication/3436206_Applications_of_Machine_Learning_to_Cognitive_Radio_Networks
29. Aspects of Machine Learning in Cognitive Radio Networks | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/322010119_Aspects_of_Machine_Learning_in_Cognitive_Radio_Networks
30. Path loss modeling based on neural networks and ensemble method for future wireless networks - PMC, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10558953/
31. Path Loss Modeling: A Machine Learning Based Approach Using Support Vector Regression and Radial Basis Function Models - Scientific Research Publishing, accessed on April 9, 2025,

https://www.scirp.org/journal/paperinformation?paperid=118065
32. Path Loss Prediction Using Machine Learning with Extended Features - arXiv, accessed on April 9, 2025, https://arxiv.org/html/2501.08306v1
33. Path loss modeling based on neural networks and ensemble method for future wireless networks - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/373726622_Path_loss_modeling_based_on_neural_networks_and_ensemble_method_for_future_wireless_networks
34. Enhancing Machine Learning Models for Path Loss Prediction Using Image Texture Techniques - - Ithaca, accessed on April 9, 2025, https://ithaca.ece.uowm.gr/journal_article/enhancing-machine-learning-models-for-path-loss-prediction-using-image-texture-techniques/
35. Performance evaluation of machine learning methods for path loss prediction in rural environment at 3.7 GHz - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/352521717_Performance_evaluation_of_machine_learning_methods_for_path_loss_prediction_in_rural_environment_at_37_GHz
36. Machine Learning-Based Path Loss Modeling with Simplified Features - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/380635077_Machine_Learning-Based_Path_Loss_Modeling_with_Simplified_Features
37. Cognitive Radio Clustering Algorithm for Swarms Using Neural Networks - DTIC, accessed on April 9, 2025, https://apps.dtic.mil/sti/trecms/pdf/AD1200510.pdf
38. DeepLoRa: Learning Accurate Path Loss Model for Long Distance Links in LPWAN, accessed on April 9, 2025, https://cse.msu.edu/~caozc/papers/infocom21-liu.pdf
39. An Intelligent Path Loss Prediction Approach Based on Integrated Sensing and Communications for Future Vehicular Networks - IEEE Computer Society, accessed on April 9, 2025, https://www.computer.org/csdl/journal/oj/2024/01/10495097/1W0tDgQvH7q
40. Spatial Signal Strength Prediction using 3D Maps and Deep Learning, accessed on April 9, 2025, https://par.nsf.gov/servlets/purl/10294826
41. Path loss prediction for air-to-ground communication links via scenario transfer technology, accessed on April 9, 2025, https://www.oaepublish.com/articles/ces.2024.55
42. Deep Learning for Path Loss Prediction at 7 GHz in Urban Environment | NIST, accessed on April 9, 2025, https://www.nist.gov/publications/deep-learning-path-loss-prediction-7-ghz-urban-environment
43. (PDF) MACHINE LEARNING-BASED PATH LOSS MODELS FOR HETEROGENEOUS RADIO NETWORK PLANNING IN A SMART CAMPUS - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/376951096_MACHINE_LEARNING-BASED_PATH_LOSS_MODELS_FOR_HETEROGENEOUS_RADIO_NETWORK_PLANNING_IN_A_SMART_CAMPUS
44. Two-Step Path Loss Prediction by Artificial Neural Network for Wireless Service Area Planning | Request PDF - ResearchGate, accessed on April 9, 2025,

https://www.researchgate.net/publication/335634525_Two-Step_Path_Loss_Prediction_by_Artificial_Neural_Network_for_Wireless_Service_Area_Planning
45. Path Loss Prediction Using Deep Learning - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/386210003_Path_Loss_Prediction_Using_Deep_Learning
46. A Machine Learning Based Approach Using Support Vector Regression and Radial Basis Function Models - Scientific Research Publishing, accessed on April 9, 2025, https://www.scirp.org/journal/papercitationdetails?paperid=118065&JournalID=1003
47. Machine Learning Techniques Based on Primary User Emulation Detection in Mobile Cognitive Radio Networks - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/22/13/4659
48. Applications of Machine Learning in Spectrum Sensing for Cognitive Radios - Scholarship at UWindsor, accessed on April 9, 2025, https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=9423&context=etd
49. Accurate Path Loss Prediction Using a Neural Network Ensemble Method - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/377172054_Accurate_Path_Loss_Prediction_Using_a_Neural_Network_Ensemble_Method
50. Path Loss Prediction Accuracy Based On Random Forest Algorithm in Palembang City Area, accessed on April 9, 2025, https://www.researchgate.net/publication/370453094_Path_Loss_Prediction_Accuracy_Based_On_Random_Forest_Algorithm_in_Palembang_City_Area
51. Artificial Intelligence Enabled Radio Propagation: Path Loss Improvement and Channel Characterization in Vegetated Environments - SciELO, accessed on April 9, 2025, https://www.scielo.br/j/jmoea/a/GRSQWsVncxmMjq6mXHYD5cH/
52. GRU-SVM Based Threat Detection in Cognitive Radio Network - PMC - PubMed Central, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC9921490/
53. Vertical Federated Learning Based Privacy-Preserving Cooperative Sensing in Cognitive Radio Networks | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/349851884_Vertical_Federated_Learning_Based_Privacy-Preserving_Cooperative_Sensing_in_Cognitive_Radio_Networks
54. Secure Federated Learning for Cognitive Radio Sensing - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/369491695_Secure_Federated_Learning_for_Cognitive_Radio_Sensing
55. Radio Environment Map Construction Based On Privacy-centric Federated Learning, accessed on April 9, 2025, https://www.researchgate.net/publication/378317744_Radio_Environment_Map_Construction_Based_On_Privacy-centric_Federated_Learning
56. A Federated Learning-Based Resource Allocation Scheme for Relaying-Assisted

Communications in Multicellular Next Generation Network Topologies - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2079-9292/13/2/390
57. Decentralized Federated Learning Over Slotted ALOHA Wireless Mesh Networking - White Rose Research Online, accessed on April 9, 2025, https://eprints.whiterose.ac.uk/id/eprint/206997/1/Decentralized_Federated_Learning_Over_Slotted_ALOHA_Wireless_Mesh_Networking%20%281%29.pdf
58. Federated Learning for 5G Radio Spectrum Sensing - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/22/1/198
59. Attacking Modulation Recognition with Adversarial Federated Learning in Cognitive Radio-Enabled IoT - Durham Research Online (DRO), accessed on April 9, 2025, https://durham-repository.worktribe.com/preview/1927062/1926211AAM.pdf
60. Radio network TETRA path loss calculation by statistical polynomial kernel radial wavelet network models for RSSI predication an - The ScienceIN Publishing, accessed on April 9, 2025, https://pubs.thesciencein.org/journal/index.php/jist/article/download/a758/477/2583
61. Advances and Open Problems in Federated Learning - arXiv, accessed on April 9, 2025, http://arxiv.org/pdf/1912.04977
62. (PDF) Radio network TETRA path loss calculation by statistical polynomial kernel radial wavelet network models for RSSI predication and comparison in undulating area - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/377129490_Radio_network_TETRA_path_loss_calculation_by_statistical_polynomial_kernel_radial_wavelet_network_models_for_RSSI_predication_and_comparison_in_undulating_area
63. Secure Federated Learning for Cognitive Radio Sensing - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2304.06519
64. Robust Aggregation for Federated Learning - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/358842974_Robust_Aggregation_for_Federated_Learning
65. [1912.13445] Robust Aggregation for Federated Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/abs/1912.13445
66. SPS Webinar: Robust Aggregation for Federated Learning | IEEE Signal Processing Society, accessed on April 9, 2025, https://signalprocessingsociety.org/blog/sps-webinar-robust-aggregation-federated-learning
67. Robust Aggregation for Federated Learning - Krishna Pillutla, accessed on April 9, 2025, https://krishnap25.github.io/papers/2019_rfa.pdf
68. A Robust Aggregation Approach for Heterogeneous Federated Learning - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/372975570_A_Robust_Aggregation_Approach_for_Heterogeneous_Federated_Learning
69. [2504.03625] Reciprocity-Aware Convolutional Neural Networks for Map-Based Path Loss Prediction - arXiv, accessed on April 9, 2025,

https://arxiv.org/abs/2504.03625
70. Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies - Zhuo Lu, accessed on April 9, 2025, https://csalab.site/getsrc/?n=papers/18sse-ml4com.pdf
71. Attacking Spectrum Sensing With Adversarial Deep Learning in Cognitive Radio-Enabled Internet of Things - Research Repository, accessed on April 9, 2025, https://repository.essex.ac.uk/33464/1/Attacking_Spectrum_Sensing_With_Adversarial_Deep_Learning_in_Cognitive_Radio-Enabled_Internet_of_Things.pdf
72. Data Poisoning Attack against Neural Network-Based On-Device ..., accessed on April 9, 2025, https://www.mdpi.com/1424-8220/24/19/6416
73. GAN-Driven Data Poisoning Attacks and Their Mitigation in ... - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2079-9292/12/8/1805
74. Efficient poisoning attacks and defenses for unlabeled data in DDoS prediction of intelligent transportation systems | Security and Safety (S&S), accessed on April 9, 2025, https://sands.edpsciences.org/articles/sands/full_html/2022/01/sands20210004/sands20210004.html
75. Adversarial Deep Learning for Over-the-Air Spectrum Poisoning Attacks - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/336904889_Adversarial_Deep_Learning_for_Over-the-Air_Spectrum_Poisoning_Attacks
76. Towards Data Poisoning Attacks in Crowd Sensing Systems, accessed on April 9, 2025, https://cse.buffalo.edu/~lusu/papers/MobiHoc2018.pdf
77. Spectrum Data Poisoning with Adversarial Deep Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/1901.09247/1000
78. Challenges and Countermeasures of Federated Learning Data Poisoning Attack Situation Prediction - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2227-7390/12/6/901
79. (PDF) Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/326213785_Adversarial_Deep_Learning_for_Cognitive_Radio_Security_Jamming_Attack_and_Defense_Strategies
80. Defense Against Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks using Machine Learning | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/362161761_Defense_Against_Spectrum_Sensing_Data_Falsification_Attack_in_Cognitive_Radio_Networks_using_Machine_Learning
81. Research on Data Poisoning Attack against Smart Grid Cyber–Physical System Based on Edge Computing - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/23/9/4509
82. AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?, accessed on April 9, 2025, http://jultika.oulu.fi/files/nbnfi-fe202102255948.pdf
83. Data poisoning: The newest threat in AI and ML - NinjaOne, accessed on April 9,

2025, https://www.ninjaone.com/blog/data-poisoning/
84. What is a Data Poisoning Attack? - Wiz, accessed on April 9, 2025, https://www.wiz.io/academy/data-poisoning
85. Data Poisoning Attacks in the Training Phase of Machine Learning Models: A Review - CEUR-WS, accessed on April 9, 2025, https://ceur-ws.org/Vol-3910/aics2024_p10.pdf
86. What Is Data Poisoning? - CrowdStrike, accessed on April 9, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/data-poisoning/
87. A Novel Prediction Model for Malicious Users Detection and Spectrum Sensing Based on Stacking and Deep Learning - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/22/17/6477
88. A Novel Prediction Model for Malicious Users Detection and Spectrum Sensing Based on Stacking and Deep Learning - PubMed Central, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC9460737/
89. Cognitive Radio with Machine Learning to Increase Spectral Efficiency in Indoor Applications on the 2.5 GHz Band - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/23/10/4914
90. LDPGuard: Defenses Against Data Poisoning Attacks to Local Differential Privacy Protocols, accessed on April 9, 2025, https://www.computer.org/csdl/journal/tk/2024/07/10415225/1U1nCeGlPfi
91. FLRAM: Robust Aggregation Technique for Defense against Byzantine Poisoning Attacks in Federated Learning - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2079-9292/12/21/4463
92. Mitigating Data Poisoning Attacks On a Federated Learning Edge Computing Network, accessed on April 9, 2025, https://par.nsf.gov/servlets/purl/10279536
93. Friendly Noise against Adversarial Noise: A Powerful Defense against Data Poisoning Attacks | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/362858689_Friendly_Noise_against_Adversarial_Noise_A_Powerful_Defense_against_Data_Poisoning_Attacks
94. Defending against Poisoning Attacks in Aerial Image Semantic Segmentation with Robust Invariant Feature Enhancement - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2072-4292/15/12/3157
95. Byzantine-Robust Aggregation for Securing Decentralized Federated Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2409.17754?
96. Asynchronous Robust Aggregation Method with Privacy Protection for IoV Federated Learning - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2032-6653/15/1/18
97. Byzantine-Robust Aggregation in Federated Learning Empowered Industrial IoT - DiVA portal, accessed on April 9, 2025, https://www.diva-portal.org/smash/get/diva2:1612809/FULLTEXT01.pdf
98. Reviewing Federated Learning Aggregation Algorithms; Strategies, Contributions, Limitations and Future Perspectives - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2079-9292/12/10/2287
99. krishnap25/RFA: Robust aggregation for federated learning with the RFA

algorithm. - GitHub, accessed on April 9, 2025, https://github.com/krishnap25/RFA
100. Robust Machine Learning Approaches to Wireless Communication Networks - Eurecom, accessed on April 9, 2025, https://www.eurecom.fr/publication/7082/download/comsys-publi-7082.pdf
101. Robust Aggregation for Federated Learning - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/338291922_Robust_Aggregation_for_Federated_Learning
102. Robust Aggregation for Federated Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/1912.13445
103. FLOW Seminar #11: Krishna Pillutla (Washington) Robust Aggregation for Federated Learning - YouTube, accessed on April 9, 2025, https://www.youtube.com/watch?v=-wNV8pbMNQk
104. www.eng.auburn.edu, accessed on April 9, 2025, https://www.eng.auburn.edu/~szm0001/papers/DCN24-adversarial.pdf
105. Adversarial Attacking and Defensing Modulation Recognition With Deep Learning in Cognitive Radio-Enabled IoT | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/376767985_Adversarial_Attacking_and_Defensing_Modulation_Recognition_With_Deep_Learning_in_Cognitive_Radio-Enabled_IoT
106. Diversity Adversarial Training against Adversarial Attack on Deep Neural Networks - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2073-8994/13/3/428
107. HyperAdv: Dynamic Defense Against Adversarial Radio Frequency Machine Learning Systems | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/386520545_HyperAdv_Dynamic_Defense_Against_Adversarial_Radio_Frequency_Machine_Learning_Systems
108. Defense against adversarial attacks: robust and efficient compressed optimized neural networks - PMC - PubMed Central, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10944840/
109. 15 Security & Privacy - Machine Learning Systems, accessed on April 9, 2025, https://mlsysbook.ai/contents/core/privacy_security/privacy_security.html
110. SoK: Security and Privacy in Machine Learning, accessed on April 9, 2025, https://oaklandsok.github.io/papers/papernot2018.pdf
111. Systematic Evaluation of Privacy Risks of Machine Learning Models ..., accessed on April 9, 2025, https://www.usenix.org/conference/usenixsecurity21/presentation/song
112. Privacy and Security in Federated Learning: A Survey - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2076-3417/12/19/9901
113. (PDF) Privacy Preservation Techniques - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/302199203_Privacy_Preservation_Techniques
114. Differential Privacy in Cognitive Radio Networks: A Comprehensive Survey -

ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/358188625_Differential_Privacy_in_Cognitive_Radio_Networks_A_Comprehensive_Survey
115. Deep Learning for Privacy Preservation in Autonomous Moving Platforms Enhanced 5G Heterogeneous Networks, accessed on April 9, 2025, https://ore.exeter.ac.uk/repository/bitstream/10871/124391/1/5G_Privacy_revise.pdf
116. Localization and Privacy Preservation in Cognitive Radio Networks - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/282750812_Localization_and_Privacy_Preservation_in_Cognitive_Radio_Networks
117. What is Data Leakage? - Wiz, accessed on April 9, 2025, https://www.wiz.io/academy/data-leakage
118. Evaluating Privacy Leakage in Split Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/html/2305.12997v3
119. [2102.13472] A Quantitative Metric for Privacy Leakage in Federated Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/abs/2102.13472
120. A Quantitative Metric for Privacy Leakage in Federated Learning - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/349682823_A_Quantitative_Metric_for_Privacy_Leakage_in_Federated_Learning
121. Machine Learning Techniques for Identification using Mobile and Social Media Data - UCL Discovery, accessed on April 9, 2025, https://discovery.ucl.ac.uk/10109672/1/thesis_corrections_20200908.pdf
122. Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks, accessed on April 9, 2025, https://nsec.sjtu.edu.cn/data/Security%20and%20Privacy%20of%20Collaborative%20Spectrum%20Sensing%20in%20Cognitive%20Radio%20Networks.pdf
123. Machine Learning-Based Full Duplex Communications and Cognitive Radio Networks - King's College London Research Portal, accessed on April 9, 2025, https://kclpure.kcl.ac.uk/portal/en/studentTheses/machine-learning-based-full-duplex-communications-and-cognitive-r
124. Systematic Evaluation of Privacy Risks of Machine Learning Models - USENIX, accessed on April 9, 2025, https://www.usenix.org/system/files/sec21fall-song.pdf
125. Can We Realize Data Freshness Optimization for Privacy Preserving-Mobile Crowdsensing With Artificial Noise? - IEEE Computer Society, accessed on April 9, 2025, https://www.computer.org/csdl/journal/tm/2024/12/10520821/1WIWF9mZIA0
126. Context-Aware CSI Tracking and Path Loss Prediction Using Machine Learning and Dynamical Systems - arXiv, accessed on April 9, 2025, https://arxiv.org/html/2407.20123v1
127. Roadmap of Adversarial Machine Learning in Internet of Things-Enabled Security Systems, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/24/16/5150
128. What Is Adversarial AI in Machine Learning? - Palo Alto Networks, accessed on

April 9, 2025, https://www.paloaltonetworks.com.au/cyberpedia/what-are-adversarial-attacks-on-AI-Machine-Learning
129. Robust Trajectory Prediction against Adversarial Attacks - Proceedings of Machine Learning Research, accessed on April 9, 2025, https://proceedings.mlr.press/v205/cao23a/cao23a.pdf
130. A Comprehensive Review of Adversarial Attacks on Machine Learning - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2412.11384
131. Why Adversarial Attacks are important in the path to human-like-AI - Medium, accessed on April 9, 2025, https://medium.com/bits-and-neurons/why-adversarial-attacks-are-important-in-the-path-to-human-like-ai-93475d0b7acc
132. Adversarial Machine Learning for NextG Covert Communications Using Multiple Antennas, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC9407147/
133. Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2005.05321
134. Adversarial Attacks and Defenses for Wireless Signal Classifiers using CDI-aware GANs - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2311.18820
135. Security evaluation techniques of Cognitive Radio Network status and challenges | Request PDF - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/363910828_Security_evaluation_techniques_of_Cognitive_Radio_Network_status_and_challenges
136. AI Driven Security Threat Analysis for 5G Cognitive Radio Short Range Applications, accessed on April 9, 2025, https://www.ijisae.org/index.php/IJISAE/article/view/7045
137. Deep Reinforcement Learning for Physical Layer Security Enhancement in Energy Harvesting Based Cognitive Radio Networks - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/23/2/807
138. Privacy Program Metrics: How to Evaluate Your Privacy Program's Effectiveness | TrustArc, accessed on April 9, 2025, https://trustarc.com/resource/privacy-program-metrics-how-to-evaluate-your-privacy-programs-effectiveness/
139. Friendly Noise against Adversarial Noise: A Powerful Defense against Data Poisoning Attacks, accessed on April 9, 2025, https://proceedings.neurips.cc/paper_files/paper/2022/file/4e81308aa2eb8e2e4eccf122d4827af7-Paper-Conference.pdf
140. Data poisoning attacks on traffic state estimation and prediction - UW Math Department, accessed on April 9, 2025, https://sites.math.washington.edu/~rtr/papers/rtr270-DataPoisoning.pdf
141. De-Pois: An Attack-Agnostic Defense against Data Poisoning Attacks - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/351592537_De-Pois_An_Attack-Agnosti

c_Defense_against_Data_Poisoning_Attacks
142. [2302.02300] Run-Off Election: Improved Provable Defense against Data Poisoning Attacks, accessed on April 9, 2025, https://arxiv.org/abs/2302.02300
143. ML Attack Models: Adversarial Attacks and Data Poisoning Attacks - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2112.02797
144. Data Poisoning Attacks Against Outcome Interpretations of Predictive Models - College of Engineering - Purdue University, accessed on April 9, 2025, https://engineering.purdue.edu/~lusu/papers/KDD2021HengtongB.pdf
145. Top 5 Outlier Detection Methods Every Data Enthusiast Must Know - DataHeroes, accessed on April 9, 2025, https://dataheroes.ai/blog/outlier-detection-methods-every-data-enthusiast-must-know/
146. Unsupervised Outlier Detection on Databricks, accessed on April 9, 2025, https://www.databricks.com/blog/2023/03/13/unsupervised-outlier-detection-databricks.html
147. Outlier detection with Local Outlier Factor (LOF) - Scikit-learn, accessed on April 9, 2025, https://scikit-learn.org/stable/auto_examples/neighbors/plot_lof_outlier_detection.html
148. Outlier Detection Methods: A General Comparison | Download Table - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/figure/Outlier-Detection-Methods-A-General-Comparison_tbl3_220459044
149. A Comprehensive Guide to Outliers in Machine Learning: Detection, Handling, and Impact, accessed on April 9, 2025, https://medium.com/@samiraalipour/a-comprehensive-guide-to-outliers-in-machine-learning-detection-handling-and-impact-f7d965bba7a5
150. Automatic Outlier Detection - AutoOD - DSpace@MIT, accessed on April 9, 2025, https://dspace.mit.edu/bitstream/handle/1721.1/150844/3588700.pdf?sequence=1&isAllowed=y
151. Advanced Outlier Detection Using Unsupervised Learning for Screening Potential Customer Returns - University of California, Santa Barbara, accessed on April 9, 2025, https://web.ece.ucsb.edu/~lip/publications/OutlierDectectionIEEE-ITC2020.pdf
152. Friendly Noise against Adversarial Noise: A Powerful Defense against Data Poisoning Attacks - Baharan Mirzasoleiman, accessed on April 9, 2025, https://baharanm.github.io/assets/pdf/liu22friendly.pdf
153. Certified Defenses for Data Poisoning Attacks - NIPS papers, accessed on April 9, 2025, http://papers.neurips.cc/paper/6943-certified-defenses-for-data-poisoning-attacks.pdf
154. Generative Adversarial Networks-Based Semi-Supervised Automatic Modulation Recognition for Cognitive Radio Networks - PMC - PubMed Central, accessed on April 9, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC6263619/

155. IASC | Free Full-Text | Generative Adversarial Networks for Secure Data Transmission in Wireless Network - Tech Science Press, accessed on April 9, 2025, https://www.techscience.com/iasc/v35n3/49418/html
156. Generative Adversarial Networks-Based Semi-Supervised Automatic Modulation Recognition for Cognitive Radio Networks - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/18/11/3913
157. (PDF) Adversarial Learning Based Spectrum Sensing in Cognitive Radio - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/356794287_Adversarial_Learning_Based_Spectrum_Sensing_in_Cognitive_Radio
158. Privacy-Preserving Detection of Tampered Radio-Frequency Transmissions Utilizing Federated Learning in LoRa Networks - MDPI, accessed on April 9, 2025, https://www.mdpi.com/1424-8220/24/22/7336
159. Deep Learning Frameworks for Cognitive Radio Networks: Review and Open Research Challenges - arXiv, accessed on April 9, 2025, https://arxiv.org/pdf/2410.23949
160. Robust and Efficient Average Consensus with Non-Coherent Over-the-Air Aggregation, accessed on April 9, 2025, https://arxiv.org/html/2504.05729v1
161. CONTRIBUTION TO PRIVACY-ENHANCING TECHNOLOGIES FOR MACHINE LEARNING APPLICATIONS a dissertation submitted to the department of t - UPCommons, accessed on April 9, 2025, https://upcommons.upc.edu/bitstream/handle/2117/331634/TAFRH1de1.pdf
162. Privacy-Preserving and Post-Quantum Counter Denial of Service Framework for Wireless Networks - arXiv, accessed on April 9, 2025, https://arxiv.org/html/2409.01924v1
163. A Survey on Machine-Learning Techniques in Cognitive Radios - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/260670884_A_Survey_on_Machine-Learning_Techniques_in_Cognitive_Radios
164. An Image-based ML Approach for Wi-Fi Intrusion Detection System and Education Modules for Security and Privacy in ML, accessed on April 9, 2025, https://hammer.purdue.edu/articles/thesis/An_Image-based_ML_Approach_for_Wi-Fi_Intrusion_Detection_System_and_Education_Modules_for_Security_and_Privacy_in_ML/25733883
165. Security and Privacy in Critical Infrastructure Cyber-Physical Systems: Recent Challenges and Solutions, accessed on April 9, 2025, https://sprite.utsa.edu/publications/dissertation/boustaniWSUEECS16.pdf
166. TOWARDS MACHINE LEARNING BASED ACCESS CONTROL - Prof. Ravi Sandhu, accessed on April 9, 2025, https://profsandhu.com/ics/2022%20Mohammad%20Nobi.pdf
167. THE IMPACT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ON ORGANIZATIONS CYBERSECURITY by Mustafa Abdulhussein Dissertation - Scholars Crossing, accessed on April 9, 2025, https://digitalcommons.liberty.edu/context/doctoral/article/6301/viewcontent/36_Abdulhussein_2C_20Mustafa_20_28L29731703_29.pdf

168. Performance Evaluation of Cognitive Radios: Metrics, Utility Functions, and Methodology - Auburn University, accessed on April 9, 2025, https://www.eng.auburn.edu/~szm0001/papers/ZhaoPROCIEEE2009.pdf
169. Performance Comparison of Machine Learning Techniques in Detection of Primary users for Cognitive Radio - GRENZE Scientific Society, accessed on April 9, 2025, https://thegrenze.com/pages/servej.php?fn=304_1.pdf&name=Performance%20Comparison%20of%20Machine%20LearningTechniques%20in%20Detection%20of%20Primary%20users%20for%20CognitiveRadio&id=2567&association=GRENZE&journal=GIJET&year=2024&volume=10&issue=1
170. Accepted Papers (Spring) - ACM WiSec 2024, accessed on April 9, 2025, https://wisec2024.kaist.ac.kr/accepted-papers-spring/
171. Railway Cognitive Radio to Enhance Safety, Security, and Performance of Positive Train Control - Federal Railroad Administration, accessed on April 9, 2025, https://railroads.fra.dot.gov/sites/fra.dot.gov/files/fra_net/2932/TR_Railway%20Cognitive%20Radio%20%20%20Final%20Report_edited-AA-JW-CO-20121205_FINAL.pdf
172. Design and Evaluation of Noise Simulation Algorithm Using MATLAB Ray Tracing Engine for Noise Assessment and Prediction - MDPI, accessed on April 9, 2025, https://www.mdpi.com/2076-3417/15/3/1009
173. Path Loss Models - INET Framework - OMNeT++, accessed on April 9, 2025, https://inet.omnetpp.org/docs/showcases/wireless/pathloss/doc/index.html
174. Dissertation Structure & Layout 101 (+ Examples) - Grad Coach, accessed on April 9, 2025, https://gradcoach.com/dissertation-structure/
175. Structuring Your Dissertation Chapters: Clearing the Path for Readers, accessed on April 9, 2025, https://falconediting.com/en/blog/structuring-your-dissertation-chapters-clearing-the-path-for-readers/
176. What Is a Dissertation? | Guide, Examples, & Template - Scribbr, accessed on April 9, 2025, https://www.scribbr.com/category/dissertation/
177. The Complete Guide to Writing a Dissertation - Grammarly, accessed on April 9, 2025, https://www.grammarly.com/blog/academic-writing/how-to-write-a-dissertation/
178. Security Assessment Reports: A Complete Overview, accessed on April 9, 2025, https://www.legitsecurity.com/blog/what-are-security-assessment-reports
179. SECURITY ASSESSMENT REPORT, accessed on April 9, 2025, https://ndlegis.gov/files/committees/67-2021/23_5011_3000appendixb.pdf
180. Chapter 11: Written Reports and Verbal Briefings. Security Analysis: A Critical Thinking Approach - Encompass, accessed on April 9, 2025, https://encompass.eku.edu/cgi/viewcontent.cgi?filename=10&article=1005&context=ekuopen&type=additional
181. How to Write a Security Officer Report (Writing Samples Inside) - Belfry Software, accessed on April 9, 2025, https://www.belfrysoftware.com/blog/security-officer-report-writing-samples
182. Privacy Inference and Defense of Machine Learning Models - Publikationen

der UdS - Universität des Saarlandes, accessed on April 9, 2025, https://publikationen.sulb.uni-saarland.de/bitstream/20.500.11880/36610/1/PhD_thesis%20%28Zheng%20Li%29.pdf
183. Secure and Private Machine Learning - Refubium - Freie Universität Berlin, accessed on April 9, 2025, https://refubium.fu-berlin.de/bitstream/handle/fub188/37279/Dissertation_Boenisch.pdf?sequence=3&isAllowed=y
184. Dissertation Topics on Data Security and Privacy - ResearchProspect, accessed on April 9, 2025, https://www.researchprospect.com/dissertation-topics-on-data-security-and-privacy/
185. (PDF) SoK: Security and Privacy in Machine Learning - ResearchGate, accessed on April 9, 2025, https://www.researchgate.net/publication/326276006_SoK_Security_and_Privacy_in_Machine_Learning
186. SoK: Towards the Science of Security and Privacy in Machine Learning - Fei Hu, accessed on April 9, 2025, https://feihu.eng.ua.edu/NSF_BD_lec11.pdf
187. ENSURING INTEGRITY, PRIVACY, AND FAIRNESS FOR MACHINE LEARNING USING TRUSTED EXECUTION ENVIRONMENTS by Aref Asvadishirehjini APP, accessed on April 9, 2025, https://utd-ir.tdl.org/bitstreams/5241412f-5d4a-49d9-818b-e35390a10f37/download
188. Informing the Design and Refinement of Privacy and Security Controls - Daniel Smullen, accessed on April 9, 2025, https://www.daniel-smullen.com/resources/Daniel_Smullen___Dissertation.pdf
189. Machine Learning for Risk Prediction and Privacy in Electronic Health Records by Eric Lantz A dissertation submitted in partial - cs.wisc.edu, accessed on April 9, 2025, https://pages.cs.wisc.edu/~dpage/lantz.dissertation.pdf
190. Dissertations / Theses: 'Security and privacy issues' - Grafiati, accessed on April 9, 2025, https://www.grafiati.com/en/literature-selections/security-and-privacy-issues/dissertation/
191. "On Security and Privacy in Machine Learning" by Thomas Cilloni - eGrove, accessed on April 9, 2025, https://egrove.olemiss.edu/etd/2746/