Statement and Confirmation of Own Work

A signed copy of this form must be submitted with every assignment.
If the statement is missing your work may not be marked.

Student Declaration

I confirm the following details:

Student Name:	Johnson Kenisha Corera
Student ID Number:	c23020001@cicra.edu.lk
Qualification:	Bachelor in Cyber Security
Unit:	SIT325 Advanced Network Security
Centre:	CICRA Campus
Word Count:	1407

I have read and understood both *Deakin Academic Misconduct Policy* and the *Referencing and Bibliographies* document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.

I confirm that I have not exceeded the stipulated word limit by more than 10%.

I confirm that this is my own work and that I have not colluded or plagiarized any part of it.

Candidate Signature:	J.
Date:	29/01/2025

Task 9.1P
Table of Content

Table of Acronyms

Acronyms	**Meaning**
IP	Internet Protocol
IDS	Intrusion detection System
RF	Radio Frequency
FAR	False Acceptance Rate
IoT	Internet of Things

Q1. In your own words, please explain a novel IDS proposed by the authors of [1].

- According to the research team's statements they introduced an innovative intrusion detection system which employs radio frequency fingerprinting methodologies to enhance network protection mechanisms within dense IoT device environments. RF fingerprinting functions through recognition of unique electromagnetic signals which devices produce while they communicate. RF fingerprints directly correlate with a device's electronic components together with its operating surroundings and experts keep these prints under this name.

- Analysis of RF signatures in this paper relied on Mahalanobi's Distance Correlation Theory as its main advantage. The comparison of signal versus profile through Mahalanobis distance measurement successfully identified any new radio frequency transmissions no matter their source between authorized devices and possible intruders. The identification system establishes genuine device tracking abilities even when attackers modify fundamental software-based identifiers such as IP addresses. The technique offers essential protection for IoT network devices that rely on fundamental security measures because their processing power is limited.

Q2. What are the advantages of RF signature-based IDS over IP-traffic based IDSs?

- IP traffic fingerprint analysis enables a distinct method compared to RF-based IDS with critical functional variations. Security boosts dramatically due to the focus on physical communication parameters as the primary benefit of IP traffic fingerprinting IDS. Traditional intrusion detection systems operating through packet analysis and traffic pattern examination encounter breaching difficulties with IP spoofing coupled with packet injection attacks. Through RF fingerprinting the system eliminates physical characteristics of signals transmitted for analysis of layers that exceed data.

- Analysis at the second level proves challenging to prevent because it depends heavily on the hardware's physical specifications which makes objective evaluation challenging. Moreover RF signature systems function by identifying attempted unauthorized communications which come through as imitations of genuine network activity of approved devices even when unapproved devices attempt entry. RF signature-based intrusion detection systems prove most effective in protecting IoT devices because these devices normally generate detectable transmission sequences and attackers can easily impersonate legitimate users when communicating with them.

Q3. What are the key evaluation metrics discussed in this research?

- The cited paper evaluates the suggested RF signature-based intrusion detection system (IDS) using three primary criteria: The evaluation of an intrusion detection system based on RF signatures examines its execution speed, false alerts and detection precision.

- The system's capacity to recognize devices and put them into correct radio bands is measured through the detection accuracy metric. A proper IDS needs to maintain consistent identification of benign from selfish devices to minimize access by untrusted entities. Evidence of the high detection rate emerges through system outcomes.

- False positive rates represent network-trend free output of devices produced by this system. Systems with as minimal FAR values as possible represent good practice for the implementation. The abbreviation 'FAR' is commonly used for this rate value. Lower false positive rates produce better IDS performance since they protect the operational integrity of actual devices and minimize overall output.

- Computational Efficiency: Indexing performance tracks both the calculated actions and the runtime duration for IDS signature evaluations that lead to final decisions. Real-time computation emerges as another consideration because most IoT devices operate with limited processing capacity yet IDS must minimize its resource utilization for practical implementation.

Q4. What are the limitations of this approach?

- This RF fingerprinting technique for intrusion detection carries several limitations despite its advantages. Due to environmental influences radio frequency broadcasts present numerous uncontrollable variables that affect their functions. Radiofrequency signals experience changes due to temperature variations along with changes in humidity thereby affecting devices with various identification properties. Signal quality continues to deteriorate and interference increases when the environment changes due to blocking objects or electrical interference.

- The system operates with a restriction of maximum simultaneous user access which prohibits scalability. ID systems storing expanded RF signature libraries for improved detection yield better results yet place heavier demands on processing capabilities and possibly degrade system performance. RF spoofing represents complex attacks that can bypass fingerprint-based systems since covert actors manipulate RF signals to form false devices which the method fails to detect. (Sood, 2022)

Q5. In the real-world how can this approach (in reference 1) be implemented and deployed? Please see Section IV of reference 2 to answer this question.

- Further development of the RF fingerprinting-based intrusion detection system's general architecture remains necessary because it requires proper integration with existing network environments to become usable for practical implementations. The first step to start the procedure involves gathering RF signatures from every authorized device which connects to the network. The IDS secures signature information which gets input during new signal analysis.

- The implementation of an IDS requires placement at network IoT gateways or wireless access points and additional sites to enable continual radio frequency spectrum monitoring. At all times the system scans incoming radio frequency signals while they are evaluated against prior wave pattern database matches to detect abnormal patterns. After identifying abnormal network signals the system tracks either automatic device block out or alerts to investigate potential security risks.

- Other elements that must be taken into account in the real-world implementation are: The RF signature database requires regular updates to include new networked devices while system modifications become necessary to adjust for changing environmental conditions. The procedures represent critical requirements which need execution consistently. The system accuracy and operation throughout time depends on essential performance review and modification procedures.

Q6. Normally, due to privacy reasons researchers are not able to get the real data sets for IDS design. Hence, sometimes they end up generating their own synthetic data sets. What is the difference between real-data set and the synthetic data sets?

- Real-world data provides extraordinarily accurate understanding of operational environments through its foundation in actual network and device measurements. These datasets provide exceptional value to IDS development and testing because they faithfully represent actual network behaviors and incidents. The acquisition of real data sets for analysis proves challenging because of data privacy requirements and regulatory limitations and the long collection periods needed as well as the potentially insufficient quality of real operational network data.

- Quasi-synthetic data represents actual information which software applications generate by mimicking natural circumstances through designed predictive models. The targeted generation of synthetic data allows researchers to handle different testing settings by creating datasets that match specific test requirements. When using synthesized data for real-world implementation there could be performance differences due to synthetic data failing to replicate unpredictable elements and real-world environments typical of operating environments.

Q7. In your opinion, how realistic are synthetic data sets?

- Realistic outcomes in synthetic data models depend to a great extent on the closeness between actual model parameters and synthetic input data parameters. IDS testing and validation benefit from high-quality synthetic data because it effectively reproduces authentic network traffic patterns according to [7]. Researchers evaluate IDS performance across different attack types and network topologies using synthesized data that model other false behavior.

- Synthetic data maintains essential differences which include its inability to replicate specific characteristics that exist within real-world data. Synthetic models lack the ability to detect anomalous interference patterns or unpredictable device breakdowns which affect system performance. The system will achieve real-world application reliability and durability through the later addition of actual data to synthetic data during evaluation. Synthetic data represents an optimal solution for both training and developmental purposes.

Q8. What type of data sets are used by the authors in [1]?

- The authors conducted evaluations with synthetic along with real datasets to validate the performance of their proposed RF fingerprinting intrusion detection system. The system's ability to detect and verify one-of-a-kind devices through their radio frequency signals was validated with actual data gathered from Internet of Things devices working within controlled areas.

- Through artificial data creation the scientists evaluated numerous attack types and environmental conditions in various simulation settings. A two-part data approach enabled the authors to properly assess the IDS system capabilities by employing synthetic data as well as genuine network intrusion samples which provided testing accuracy in routine and stressful situations. The cross-section analysis of system performance and development areas enabled by this technique proved to be an extremely advantageous method. (Nguyen, 2022)

References

- Physical Layer–Assisted Intrusion Detection System in 5G-IoT Networks, https://www.techrxiv.org/doi/full/10.36227/techrxiv.19083404.v1

- RF Fingerprinting-Based IoT node Authentication using Mahalanobis Distance Correlation Theory https://ieeexplore.ieee.org/document/9758067