12-2021

Machine Learning Application for Mission Data Reprogramming

Paolo A. Bingham

MACHINE LEARNING APPLICATION FOR MISSION DATA REPROGRAMMING

THESIS

Paolo A. Bingham, Captain, USAF

AFIT-ENV-MS-D-041

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENV-MS-D-041

MACHINE LEARNING
MISSION DATA REPROGRAMMING

THESIS

Presented to the Faculty

Department of Systems Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Systems Engineering

Paolo A. Bingham, BS

Captain, USAF

November 2021

AFIT-ENV-MS-D-041

MACHINE LEARNING
MISSION DATA REPROGRAMMING

Paolo A. Bingham, BS

Captain, USAF

Committee Membership:

Dr. Brent T. Langhals
Chair

Lt Col Paul M. Beach
Member

Lt Col Warren J. Connell
Member

Abstract

Before entering a conflict or theater, USAF aircraft require updated mission data software reprogramming. Mission data controls all electronic warfare (EW) operations of the aircraft. EW operations include identifying and jamming radar operated systems, whether they are friendly or hostile. The process of reprogramming software is continuous and routinely updated for every EW system annually. On specific circumstances, the process can be expedited to months, but this puts a strain on the development team and shifts all attention to one specific mission data file. Unfortunately, a growing number of requests to upgrade mission data to a higher priority state, has created a backlog in the reprogramming process. The result is that now many requests are delayed or simply rejected.

Successful reprogramming requires a mission data developer first categorize the radar emitter. This process involves matching all radar signal parameters to a known signal. This research developed a method to use machine learning data processing to assist in the reprogramming of mission data. Using a mission data processing algorithm, this research demonstrated how the development team can acquire a precise identification of a radar emitter by allowing the categorization to be performed by machine learning.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Brent Langhals, for his guidance and support throughout the course of this thesis effort. The insight and experience was certainly appreciated. I would, also like to thank my leadership and Commander, Lt Col Michael Deaver, for allowing me the bandwidth to pursue my academic goals.

Paolo A. Bingham

Table of Contents

Page

Abstract……..iv
Acknowledgements……v
Table of Contents……vi
List of Figures viii
List of Tables ix
I. Introduction 1
General Issue.....1
Current MD Reprogramming Process and Cycle 2
SME MD Reprogramming Background 3
Problem Statement 4
Research Objective .....**Error! Bookmark not defined.**
Investigative Questions 5
Methodology 5
Assumptions/Limitations 5
Summary 6
II. Literature Review 7
Chapter Overview 7
Radar Operations 7
MD Reprogramming Guidance.....8
Previous Efforts on Cognitive Reprogramming 10
Understanding K-Nearest Neighbor 13
Summary 14
III. Methodology 15
Chapter Overview 15
Test Dataset Creation.....15
Data Collection 17
Test Dataset Questionnaire 17

R Data Processing Results 20
Summary 24
IV. Analysis and Results 25
Chapter Overview 25
Results 25
Dataset Relevance 25
Identification Comparison 28
Summary 31
V. Conclusions and Recommendations 32
Chapter Overview 32
Conclusions of Research 32
Significance of Research 33
Recommendations for Action 34
Recommendations for Future Research 34
Appendix 35
Bibliography 46

List of Figures

Page

Figure 1. MD Reprogramming Process 2

Figure 2. Test Dataset Preview 16

Figure 3. Questionnaire Part 1 18

Figure 4. Questionnaire Part 2 18

Figure 5. Questionnaire Part 3 20

Figure 6. RStudio Code Load 21

Figure 7. RStudio Dataset 21

Figure 8. RStudio Code Normalize 22

Figure 9. RStudio Code KNN 23

Figure 10. RStudio Results Code 23

Figure 11. RStudio Results Matrix 24

Figure 12. Question 2 Results 26

Figure 13. Question 3 Results 26

Figure 14. Question 4 Results 28

Figure 15. Question 5 Confidence 30

List of Tables

Page

Table 1. Question 5 Results 29

MACHINE LEARNING

MISSION DATA REPROGRAMMING

I. Introduction

General Issue

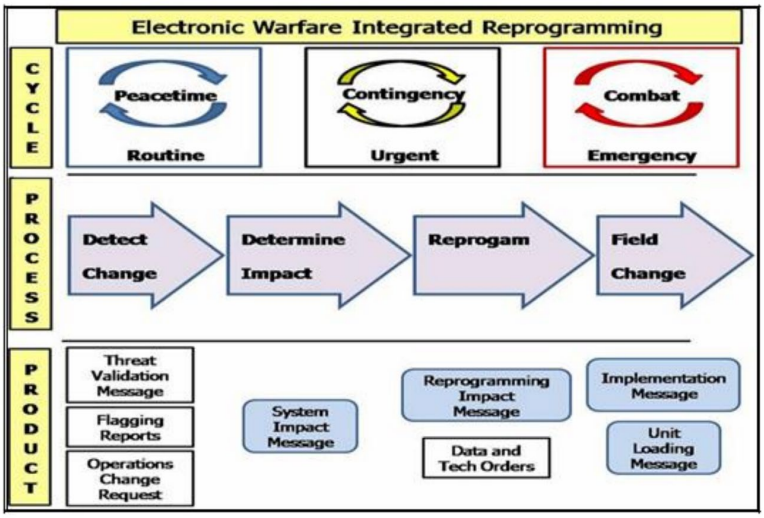
The rising need for updated operational military aircraft software creates a supply and demand imbalance where there is just one organization creating updated software and several units of various platforms, containing a handful for subsystems, demanding frequent updates to perform their missions. Considering that human lives are at stake, this organization cannot decline any request but, due to manning and funding, is forced to prioritize their production of software. The tempo that the engineers are operating under is extremely taxing and the software product can suffer. There may be ways to optimize this process by allowing machine learning to assist in this task and this research aims to prove that is possible.

Mission Data (MD) is the software programming of Electronic Warfare (EW) subsystems. The software provides various results based on the system that is utilizing it. For example, a Radar Warning Receiver uses MD to identify a threat and a radar jammer uses it to employ an appropriate countermeasure. The 53rd Electronic Warfare Group at Eglin Air Force Base, Florida, is tasked with being the sole provider of Electronic Warfare Mission Data for the U.S. Combat Air Force (CAF) in accordance with AFI 10-703 [1]. This means supplying the entire fleet of U.S. CAF platforms with frequent updates to any subsystems that use EW to attack, protect against, and identify an enemy threat. These subsystems all use unique MD computers that create specific updates for

each subsystem and are not interchangeable. Due to this fact, the 53EWG must equip each subsystem with its specific software load, test equipment, training software, and subject matter experts (SME) to support only one subsystem.

Current MD Development Process

Once a new threat emerges within an area of responsibility (AOR), intelligence collection agencies analyze new parametric data and determine if this data belongs to a friendly, adversary, neutral or commercial system. This analysis is needed to properly categorize parametric data (frequency, pulse repetition interval, pulse width, etc) into their appropriate signal sources. The 53EWG then determines the impact of the new signal source in the AOR and recommends to either take no action or reprogram. Using this recommendation, operational units can then task the 53EWG to perform the MD reprogramming process. Finally, the reprogrammed MD is sent to the operational units for fielding. This sequence of events can be found in AFI 10-703 and Figure 1 below will help illustrate using the process section.



AFI 10-703 also determines expected timelines for each MD delivery [1]. Any EW subsystem can support several AORs and a dedicated MD is expected to separate them apart of other AORs for the same EW subsystem. Routine reprogramming is expected for all AORs of each subsystem annually. However, depending on the request, these tasks can rise to Urgent or Emergency priority levels. Tasks in this category have an expedited timeline from 24 to 72 hours, further increasing the strain on the SME to process MD.

SME MD Reprogramming Background

Regardless of the tasking priority level, the SME conducts similar procedures to reprogram MD. Using the parametric data collected by the intelligence agencies, the SME of a specific EW subsystem enters each new threat data into their subsystem's MD database. Parametric data includes threat name, operating mode, frequencies, pulse repetition intervals (PRI), and pulse width (PW), among others. Real world MD databases include several parameters and different subtypes of those parameters. However, this research will focus on a select amount of parameters which will be assessed by SME. An example of this database created by the research team can be found in the Methodology section of this thesis.

Once threat data is entered into the MD database, the SME then decides how to program the EW subsystem to categorize incoming radar signals and match the programmed database. For example, a radar signal with a specific frequency, PRI and scan rate will have a matching database entry which can be categorized to be displayed for situational awareness or employ jamming against the threat. However, there are cases

when the radar signal matches multiple entries and the SME must choose which identification to display or threat to attempt to employ countermeasures against.

Problem Statement

Our adversaries continue to develop systems that threaten the safety of our aircrew, while the speed in which EW identification and countermeasures are updated is too slow to ensure high aircrew survivability, especially given the level of threat complexity makes it increasingly difficult to rapidly produce MD. Additionally, the increasing tension in international conflicts increases the demand for updated software to counter any situation. Given these circumstances, the current way MD is produced is not sustainable. Incorporating a data processing tool to the MD reprogramming process could reduce the SME workload prior to fielding. The primary obstacle for this process is that AFI 10-703 requires “rapid detection, accurate identification and appropriate response” [1] and the decision making for accurate and appropriate responses needs a human in the loop to accomplish.

Research Objective

This research seeks to answer the following questions:

1) Can a data processing tool using a machine learning algorithm be used to categorize a threat using a mission data dataset?

2) It is possible to create a categorization algorithm that would use existing mission data datasets to identify an unknown emitter?

3) If it is possible, can the machine learning algorithm match what a SME would identify the new emitter as?

Investigative Questions

In order to answer the research question above, we need to ensure that the reprogramming task presented to SME's from the 53EWG remains operationally representative. To achieve this, the following questions must also be answered.

- Is the research test dataset representative to an operational dataset?
- Are the results of the data processing tool comparable to those of SMEs?

This test dataset will need to be validated by SMEs to verify it closely resembles an actual mission data dataset. Additionally, the results of the data processing will be compared with those given by SMEs to determine if the data processing tool can achieve acceptable categorization.

Methodology

This research will focus on the reprogramming process only and will exclusively be tied to EW. The hypothesis is that a data processing tool can be used to categorize an emitter using parametric sets. The data will be gathered by creating a test dataset of emitter parametrics and running a data processing algorithm against the database. A detailed explanation of the methodology can be found in Chapter III.

Assumptions/Limitations

This research will use a simple test dataset to prove the concept of comparing data processing tool results to the results of SME identifications. A test dataset will remove the potential of this research become classified. Association of unclassified parametrics or threat performance can result in a security infraction. This test database will only use public or commercial radar parameter guidance. Using a classified dataset with accurate

parametric information would ensure that the emitter complexity for future considerations of this research within classified networks. Additionally, all hypothetical Pulse Repetition Intervals (PRI) are fixed. PRIs come is three configurations fixed, patterned and randomized. A fixed PRI remains stable while a radar transmits it. Patterned PRI transmits in a sequence of stable PRIs. Randomized PRI fluctuates during transmission in a randomized pattern. Following the classification limitation above, this research will adhere to fixed PRIs to maintain this document unclassified.

Summary

The MD production process places high demand on the 53EWG. The reprogramming phase can take as long as a year to complete. A data processing tool using a machine learning algorithm could help expedite this process. This research aims to provide a possible solution utilizing previous developments on computer-based MD processing and 53EWG SME feedback. In order to maintain the unclassified classification of this research, all hypothetical examples of MD used in this research with use public radar operation guidance and limit association to operational MD parametrics.

II. Literature Review

Chapter Overview

This research will leverage information from several published articles. The review was split into four parts; radar operations, MD reprogramming guidance, current or previous efforts on cognitive reprogramming, and understanding machine learning data processing tools. The goal of this section is to highlight the connections to our research. Machine learning or cognitive EW is not a new concept but it can be refined.

Radar Operations

This research uses a test dataset of hypothetical threats and parametrics such as frequency, pulse repetition intervals and pulse width. These threats are then identified by a Radar Warning Receiver (RWR) system on the aircraft. This section will provide background information on how radar emitter or threat works and how a RWR system detects and identifies the threat.

A Surface to Air Missile utilizes a fire control radar to "provide information such as target azimuth, elevation, range and velocity in order to calculate a firing solution" [2]. These radars types can operate in multiple modes such as search or track. In search mode, the radar performs sweeps of a specific sector with a wider beam to locate the target. Once the target is located, the radar operator may switch to track mode. During the tracking phase, the radar will use a narrower beam directly on the target. Fire control radars have a transmitting and receiving component [2]. The transmitter sends pulses with the attuned frequency towards the target. The receiver collects the radar returns after the transmitted pulses echo back to the radar. The pulses that are transmitted create the

target location information listed above needed to calculate the firing solution. “Typical continuous tracker radar characteristics include a very low pulse repetition interval, a very narrow pulse width, and a very narrow beamwidth. Using one of several possible scanning techniques, the radar system automatically follows all target motions” [3]. This describes the minimum test parametrics needed to identify an emitter: frequency, pulse repetition interval, pulse width, and scan rate.

Detecting a radar signal from an aircraft can be accomplished using a radar warning receiver (RWR). The ALR-56M is a common example of RWR equipped on all F-16s [4]. The ALR-56M is a super heterodyne receiver which “continuously detects and intercepts radio frequency signals” by scanning specific frequencies [4]. These signals are then stored and processed to identify the pulse repetition interval and pulse width used by the detected radar.

The primary role and responsibility of the 53EWG is to develop all MD for the CAF. MD are “files a computer uses to perform signal discrimination, target a threat, or elicit jammer responses" [1]. Using the example of the ALR-56M above, MD is the programming that uses frequency, pulse repetition interval and pulse width to identify a signal. A RWR with the proper MD will process the signal data and display to the aircrew the programmed identification.

MD Reprogramming Guidance

The problem statement of this research highlights that the current MD production process is not sustainable. Air Force Instruction 10-703 places all responsibility of MD reprogramming on the 53EWG [1]. The AFI provides a detailed sequence of phases once

a new threat is discovered from the EW reprogramming process. The steps are detect change, determine the impact, reprogram, and field change. Detect change involves US Intelligence Agencies gathering signal data of new threats. This data is provided to 53EWG for analysis. Determine impact phase includes the 53EWG's analysis of new intelligence data, which is used to determine how the new signal affects currently fielded MD. The reprogram phase involves editing MD software to reflect the new data, perform regression testing to verify previous programmed are identified as intended, and testing new changes for results. Finally, the field change phase is the process when the finalized and tested MD software is formatted for loading onto the aircraft, tested, and distributed to operational units.

Regardless of impact, the 53EWG is required by AFI to accomplish all steps in this process. Depending on the impact assessment in step two, the reprogramming team is given from 24 hours to 72 hours for high priority requests and up to one year for all routine reprogramming updates [1]. This research aims to prove that this process can be expedited by machine learning and facilitate the reprogram phase. The reprogramming phase constitutes the longest portion of MD production as determined by the timelines above. MAJCOMs requesting MD prioritize the order in which files are produced based on threats or survivability creating a queue. An expedited reprogramming phase would greatly shorten this queue and allow reprogramming of all needed MD files, whether high priority or routine, without needing prioritization. The need to ensure higher survivability rates of aircrews in contested environments calls for innovative methods to provide electronic protection.

Previous Efforts on Machine Learning Radar Identification

Machine learning for EW is not a new concept. However, it is a concept that is still evolving and requires more research. Kuzdeba and Radlbeck provide an early look on the concept of Cognitive EW in their work, "Performance Metrics for Cognitive Electronic Warfare – Electronic Support Measures". The goal of their research was to create a framework for performance metrics to rate cognitive EW. Their work began by first defining and explaining Electronic Support Measures. ESM "understand the RF environment and provide emission intercept, detections, identification, characterization, location, and overall situational awareness of emitters" [8]. Similarly to our research, they explain that current systems rely on preprogrammed databases to perform ESM. Although not mentioned in their research explicitly, we know they are referring to MD. The document then introduces the concept of Cognitive ESM and describes it as a method of using "both prior knowledge and learning through environment observations" to perform EW tasks [8].

The framework they developed to rate ESM performance included five metrics; accuracy, timeliness, completeness, brevity, and efficiency. These metrics were derived for the primary goal of providing situational awareness. However, they clarify these metrics are not meant to be compared with a non-cognitive system. The reasoning is that a non-cognitive system being already preprogrammed to detect specific threats is not comparable to a cognitive system attempting to categorize new threats [8]. After establishing the framework and defining each metric, the paper sets up for an analysis of this system once it is realized.

The second relevant research builds upon the concept of cognitive EW and adds the objective of choosing a jamming technique. In “Research on Decision-making System of Cognitive Jamming against Multifunctional Radar”, Zhang and Zhu performed a study on using cognitive EW to combat the continuous development of new radar systems. Due to threat emitters having several operational modes, “it is impossible to establish one-to-one correspondence” [9]. Their research highlights recent developments by Defense Advanced Research Projects Agency (DARPA) to develop cognitive jamming to counter the rapid increase of radar systems and develop the Next Generation Jammer (NGJ) to cognitively select jamming strategies. The traditional jamming strategy selecting system intercept a signal, processes the signal and matches it against a jamming method database [9]. Again, while not explicitly named, the jamming method database is an example of MD.

Zhang and Zhu’s research here introduces the concept of cognitive jamming decision-making system. The system involves a case diagram, where the incoming radar signal is analyzed and matched against the jamming method database as traditionally done. If the programmed signal exists, employ the jamming technique. However, if the signal is not included in the database, utilize machine learning to determine the appropriate technique [9]. The paper concludes by stating the goal was to put forward the emphasis of cognitive EW and reiterating the importance of studying decision-making systems for cognitive jamming.

The third and last research not only shows the concepts presented above but also builds on them to perform experiments using machine-learning algorithms for EW. Compared to our research, a similar research effort on using machine learning was

performed by Kang and Park on their published work, “Autonomously Deciding Countermeasures against Threats in Electronic Warfare”. The aim of their study was to not only identify a new threat using machine learning but to also employ an appropriate countermeasure depending on the threat and if there was an engagement against the aircraft [5]. The first main difference from their research and ours is that while theirs focuses on machine learning assisting the aircrew during flight, ours research focuses on assisting reprogramming teams to produce MD efficiently.

Similarly, the first step in Kang and Park’s research is defining what a threat is and the determining the data or parametrics needed to test the machine learning algorithm. The parameters used for their research were taken by analyzing the APR-39 RWR system resembling our use of the ALR-56M to include frequency, pulse repetition interval, pulse width, and pulse power [5]. Using these parameters for detection, the next step is threat classification. In the last step, our research approaches deviate as Kang and Park employ machine learning in an attempt to have the algorithm decide on an appropriate countermeasure while on-board of the aircraft (as opposed to the objective of this research which is to provide updated MD).

After determining the parameters needed, Kang and Park chose the machine learning algorithm. The algorithm used was Decision Tree and the processing tool used is called WEKA. After loading their training dataset to the data processing tool and running the algorithm, they categorized the target sets.

Lastly, after categorizing, it came time to choose a countermeasure. Kang and Park chose to form a list of scenarios depending on the categorizations. The identified

threats would fall into categories of radar warning or missile warning. Based on those results, the algorithm would decide between chaff, flare, or jamming as the appropriate countermeasure. The experiment consisted of thirty trials using three strategies of countermeasure selection. The strategies were selection of countermeasure with highest utility, selection of countermeasure with success rate, and random selection. The results showed selecting the countermeasure with highest utility had an increased performance of 15.81% over the other strategies [5].

Understanding K-Nearest Neighbor

This research uses a hypothetical dataset as the programmed MD and it needs a machine learning algorithm that uses the dataset as a reference for new data. A supervised algorithm relies on already categorized data similar to the threats in the dataset. K-Nearest Neighbor (KNN) is a supervised algorithm that is primarily used for classification which is the exact outcome this research aims for. KNN algorithms work by selecting categorized data as a training set then by comparing uncategorized data to similar records in the training set, the algorithm will attempt to classify this data [6]. KNN also allows for weighting of the training set variables. If a variable is deemed more important, weighting will account for those higher priority variables over those not weighted [6]. Considering the research gathered when selecting the threat parameters to use to identify MD, weighting favoring those parameters of higher importance should be beneficial in this research. The last consideration in using KNN is in choosing the right K value. K represents the number of nearby neighbors the algorithm will attempt to match [6]. This research will assume a K value between 10 and 20 in order to account for

multiple test dataset points.

53EWG SME's could use an algorithm like KNN to expedite the MD reprogramming process. Identification of new parametric data could be performed by KNN and MD SME's would then confirm the identification made by the algorithm or have the option to edit to one of their choosing. An algorithm that categorizes new parameter sets by comparing to nearby data points already in the dataset, the SME would assume the algorithm chose the closest existing values. This would expedite the verification process by giving the SME an identification made by relating to similar data entries.

Summary

This research focuses on radar threats and the example of fire control radars defines the RF signals used to locate, track and guide weapons towards targets. RWRs detect these RF signal and after analyzing the signal, provide situational awareness to the aircrew using the RF signal parametrics to identify the threat. Due to AFI mandates, the 53EWG is overtasked and their involvement in the MD process can add up to a year per MD software file. The phases of reprogramming show potential areas where and machine-learning tool could expedite the process. Cognitive EW as a concept is not new but it is still in development and more application research is needed. However, there is some research showing the potential of using machine-learning for countermeasure selection. KNN is proposed as a suitable approach for MD identification. Utilizing nearby data points to categorize new parameter sets could help SME's shorten the MD development cycle.

III. Methodology

Chapter Overview

This chapter will highlight the methods used to develop this research. The purpose is to provide a detailed framework of how the data was collected and the sources used to generate this research. A control test dataset was required to perform this research and the steps to create it are detailed in Test Dataset Creation below. The primary sources of data were the test dataset questionnaires and R data processing results. The following sections under Data Collection will describe the steps taken to gather this data. Following the Data Collection, Chapter IV will cover the analysis of all data.

Test Dataset Creation

The first step to perform this research was creating a test dataset. This test dataset was made using Excel and populated with hypothetical radar emitter data or parametrics. The radar emitters were identified on the spreadsheet rows as four threats; Surface-to-Air X (SA-X), SA-Y, Air Interceptor (AI-X) and AI-Y . The parametrics and threats are located in the columns. The identifying parameters are Frequency, PRI, Pulse Width, Power, and Scan Rate. The chosen parameters were selected to create enough criteria to differentiate and categorize each emitter. These choices were assessed through the questionnaire later detailed in this section. An example of the test dataset is shown below in Figure 2.

	Threat	Mode	Frequency	PRI	Pulse Width	Power	Scan Rate
2	SA-X	search	10631	189	15	90	20
3	SA-X	search	10738	177	13	90	15
4	SA-X	search	10394	178	11	90	11
5	SA-X	search	10641	115	13	90	15
6	SA-X	search	10325	104	13	90	20
7	SA-X	search	11998	154	14	90	15
8	SA-X	search	11192	188	13	90	17
9	SA-X	search	11178	199	15	90	16
10	SA-X	search	10093	160	10	90	12

Figure 2. Test Dataset Preview

The dataset contained a total of 250 rows of hypothetical radar emitter parametrics for all four emitters. Each emitter was split into up to three modes; search, track, and guide. Now with a total of eight emitter/modes combinations, data for the remaining parameters was populated. This was done by arbitrarily selecting a minimum and maximum for each parameter for each emitter/mode combination. The frequency limits were selected by matching similar radar types with an average frequency of 9100MHz [7]. This sample radar also has a maximum PRI of 300µs and a minimum PW of 0.25µs. Power (measured in dB) and scan rates (measured in seconds) were selected using previous experience in radars. The bounds above helped us determine the limits for all test dataset parameters. Frequencies from 2000MHz to 16000MHz were chosen to resemble the 9100MHz average. PRI of 1µs to 200µs and PW of 1µs to 15µs were again chosen to mimic sample limits. Using these limits, the dataset was constructed to capture enough samples all four hypothetical emitters as 250 rows of data would provide sufficient representation for these minimums and maximums.

Data Collection

Test Dataset Questionnaire

Following the test dataset creation, a questionnaire was developed to validate the efficacy of the dataset, determine the importance of the selected parametrics and create a desired outcome of five new entries to the dataset. To achieve all these goals, the questionnaire and test dataset were sent to a total of fourteen SME's in MD reprogramming, with nine responding. The SMEs belong to the 53EWG, which by AFI requirement, is the organization responsible for MD testing, production and fielding [1]. Validation on the test dataset hinged on SME expertise in MD reprogramming. Although, other organizations have members with expertise in threat parametrics, these did not have the MD reprogramming experience to answer these questions. This questionnaire had a total of five questions and the reasoning behind each is explained below. The analysis of the results will be covered in Chapter IV.

The first three questions were created to determine the validity of the test dataset. Question 1 asked the SME for their years of experience and duty title. This information was used to verify the SMEs were in fact experts in the study domain. Question 2 asked "Does the provided Mission Data database properly represent an operational database by using hypothetical threat parametrics?" and asked the SME to answer in a scale from "Strongly Agree" to "Strongly Disagree". The responses were then converted to a scale from 5 to 1 respectively and the average of these scores will determine the overall rating of the dataset. Question 3 asked "Does the provided Mission Data database use enough types of parametrics (frequency, pulse width, pulse repetition interval, etc.) to identify a threat or type of threat? If not, please use the space provided to include additional parameters" and once again asked to rate on a scale from "Strongly Agree" to "Strongly Disagree". A snapshot of the first three questions are below in Figure 3.

1. Please provide the following information.

Name:

Duty Title:

Years of Experience:

2. Does the provided Mission Data database properly represent an operational database by using hypothetical threat parametrics?

Strongly Agree Agree Neutral Disagree Strongly Disagree

3. Does the provided Mission Data database use enough types of parametrics (frequency, pulse width, pulse repetition interval, etc) to identify a threat or type of threat? If not, please use the space provided to include additional parameters.

Strongly Agree Agree Neutral Disagree Strongly Disagree

Additional Parameters Needed:_____

Figure 3. Questionnaire Part 1

Question 4 asked the SME to rate the level of importance of each of the parameters used in the test dataset from 1 to 5. The purpose of this question was to determine if the chosen parameters were appropriate. The average of these ratings was calculated and will be used in future iterations of this research to determine weighting or parameter choices. A snapshot of Question 4 is shown below in Figure 4.

4. From the provided parametrics, please rate how important each type of parametric is to identifying a threat with 5 given to very important and a 1 to those not important.

a. Frequency:	1	2	3	4	5
b. Pulse Repetition Interval:	1	2	3	4	5
c. Pulse Width:	1	2	3	4	5
d. Power:	1	2	3	4	5
e. Scan Rate:	1	2	3	4	5

Figure 4. Questionnaire Part 2

Finally, Question 5 asked the SME to use twenty-five sets of new parametrics and attempt to identify which emitter and/or emitter/mode combination it belongs to. The purpose of this question was to compare SME results to the outcome of the KNN

machine learning algorithm. For each of the twenty-five sets, a specific number for each of the five parameters was chosen. These numbers fell within the minimum and maximum limits described in the dataset creation section. The result was a new record which would point to a specific emitter. The only exception was record C which has a PRI above the expected SA-X track limit. This was deliberate as a way to confirm if our the KNN algorithm would choose to categorize an unknown set the same as the SME. Each question asked the SME to categorize the set as one of the emitters in the dataset and provide a confidence level in their response. The most common response for each question and average confidence level was recorded for each set. The success criteria for this question is whether the accuracy results found in Question 5 match the KNN accuracy results found using RStudio. Details on finding RStudio KNN accuracy will be explained in this chapter and will be analyzed in Chapter IV. A snapshot of Question 5 and the first five parameter sets is shown below in Figure 5.

5. Using the provided Mission Data database, please identify the following threats and rate your confidence on each answer with a 5 for very confident and a 1 for not confident.

a. Frequency: 7777	PRI: 190	PW: 12	Power: 90	Scan: 3	
Answer:_____					
Answer Confidence:	1	2	3	4	5
b. Frequency: 14444	PRI: 7	PW: 2	Power: 85	Scan: 0	
Answer:_____					
Answer Confidence:	1	2	3	4	5
c. Frequency: 7935	PRI: 324	PW: 15	Power: 90	Scan: 6	
Answer:_____					
Answer Confidence:	1	2	3	4	5
d. Frequency: 3333	PRI: 158	PW: 11	Power: 90	Scan: 0	
Answer:_____					
Answer Confidence:	1	2	3	4	5
e. Frequency: 15800	PRI: 97	PW: 10	Power: 85	Scan: 20	
Answer:_____					
Answer Confidence:	1	2	3	4	5

Figure 5. Questionnaire Part 3

R Data Processing Results

For this research, we used RStudio as the data processing tool and the K-nearest neighbor (KNN) machine learning algorithm to categorize our twenty-five parameter sets asked in the questionnaire to the SMEs. This section will explain the R code used to categorize the sets and perform this research. Figure 6 shows the code used to load the dataset to RStudio.

```
#Machine Learning Mission Data

#load data
setwd("C:/Datasets")

paraset <- read.csv("Parametrics3.txt")
#extract parameters without test parameter rows 251-275 for
#analysis prior to KNN algorithm
para <- paraset[1:250,]

#Open dataset and display the data

View(para) # To display the whole dataset, type the dataset name


```

Figure 6. RStudio Code Load

Parametrics3.txt is the name of the dataset and it is located in the local C Drive of the computer performing the analysis. The dataset was modified to include the twenty-five parametric test sets from the SME questionnaire. The dataframe, paraset, includes all 250 original parameter rows and the twenty-five additional test sets. The dataframe para extracts only the original parameters without the additional sets. View(para) is used to confirm that the dataset was properly loaded and should have matched Figure 2 and it is shown below in Figure 7.

	threat	mode	freq	pri	pw	type	power	scan
1	SA-X	search	10631	189	15	surface	90	20
2	SA-X	search	10738	177	13	surface	90	15
3	SA-X	search	10394	178	11	surface	90	11
4	SA-X	search	10641	115	13	surface	90	15
5	SA-X	search	10325	104	13	surface	90	20
6	SA-X	search	11998	154	14	surface	90	15
7	SA-X	search	11192	188	13	surface	90	17
8	SA-X	search	11178	199	15	surface	90	16
9	SA-X	search	10093	160	10	surface	90	12
10	SA-X	search	11014	107	12	surface	90	10

Figure 7. RStudio Dataset

Once verified that the dataset had properly loaded, the dataset was normalized using only the columns with predicting parameters (columns 2-7) to ready it for KNN processing and shown in Figure 8

```
17 ################################Normalize#########################
18
19 ##the normalization function is created
20 nor <-function(x) { (x -min(x))/(max(x)-min(x))   }
21 ##normalization function is created using full set rows 1 to 275
22 para_nor <- as.data.frame(lapply(paraset[,c(2,3,4,6,7)], nor))
23
```

Figure 8. RStudio Code Normalize

After normalizing the dataset, the data is ready for KNN processing. It begins by extracting the normalized predicting parameter columns as a training set called para_train. The actual predicting test parameters that were used to categorize were extracted as para_test. The target training set that the algorithm used to categorize the predicting training set was para_target. Finally, the test target set the algorithm categorized was test_target. Running the KNN algorithm using these sets, populated test_target as the categorized results for the new test sets included to the dataset. The code for the KNN data processing is shown in Figure 9.

```
################################KNN ANALYSIS#######################

##training dataset extracted, all row but the 25 test rows
para_train <- para_nor[1:250,]
##test dataset extracted, the 25 test rows
para_test <- para_nor[251:275,]

# also convert ordered factor to normal factor
para_target <- as.factor(paraset[1:250,1])
# the actual values of 2nd column of testing dataset to
#compare it with values that will be predicted
# also convert ordered factor to normal factor
test_target <- as.factor(paraset[251:275,1])

##run knn function
library(class)
pr <- knn(para_train,para_test,cl=para_target,k=10)

```

Figure 9. RStudio Code KNN

A confusion matrix was created to view and analyze the results of the KNN algorithm. Additionally, we used the accuracy function shown in Figure 10 to confirm the results from the confusion matrix are accurate. The output of both of these operations is shown in Figure 11. The confusion matrix output displays the possible categorizations for each of the twenty-five test sets using the KNN algorithm. The algorithm successfully categorized each with little error. This error is stems from the choice of K and near neighbors used to determine the identification. The output of the accuracy function used on the matrix, yields an accuracy of 92%. This result will be compared against the SME accuracy found using the questionnaires in Chapter IV.

```
################################Check Results#########################

##create the confusion matrix
tb <- table(pr,test_target)
tb

##check the accuracy
accuracy <- function(x){sum(diag(x)/(sum(rowSums(x)))) * 100}
accuracy(tb)
```

Figure 10. RStudio Results Code

```
              test_target
pr             AI-X guide\t AI-X track\t AI-Y guide\t AI-Y track\t SA-X guide\t
  AI-X guide\t            2            0            1            0            0
  AI-X track\t            0            2            0            0            0
  AI-Y guide\t            0            0            1            0            0
  AI-Y track\t            0            1            0            3            0
  SA-X guide\t            0            0            0            0            2
  SA-X search\t           0            0            0            0            0
  SA-X track\t            0            0            0            0            0
  SA-Y guide\t            0            0            0            0            0
  SA-Y search\t           0            0            0            0            0
  SA-Y track\t            0            0            0            0            0
              test_target
pr             SA-X search\t SA-X track\t SA-Y guide\t SA-Y search\t SA-Y track\t
  AI-X guide\t             0            0            0             0            0
  AI-X track\t             0            0            0             0            0
  AI-Y guide\t             0            0            0             0            0
  AI-Y track\t             0            0            0             0            0
  SA-X guide\t             0            0            0             0            0
  SA-X search\t            3            0            0             0            0
  SA-X track\t             0            2            0             0            0
  SA-Y guide\t             0            0            3             0            0
  SA-Y search\t            0            0            0             3            0
  SA-Y track\t             0            0            0             0            2
>
> ##check the accuracy
> accuracy <- function(x){sum(diag(x)/(sum(rowSums(x)))) * 100}
> accuracy(tb)
[1] 92
```

Figure 11. RStudio Results Matrix

Summary

The Test Dataset was created to resemble an operational dataset, using hypothetical numbers to populate it. Using questionnaires and the expertise of SME in the field of mission data, this research will validate the test dataset is relevant and identify twenty-five new parametric sets. Using the test dataset in RStudio, the KNN algorithm was able to identify the new parametric sets. The accuracy in the KNN results was 92% and it will be compared to SME questionnaire results in Chapter IV.

IV. Analysis and Results

Chapter Overview

Following the Data Collection methodology in Chapter III, this research can begin analyzing the data in the questionnaires and compare to the R data processing results. The questionnaires were used to validate the relevance on the dataset used in our data processing tool. Additionally, it was used to categorize five specific parametrics sets by the SME's. Finally, these five categorization are compared to the R processing tools categorization of the same parametric sets.

Results

Dataset Relevance

Questionnaires were sent to fourteen and received by a total of nine SMEs in mission data reprogramming. The first three questions of the questionnaires are designed to confirm the relevance of the provided dataset from the perspective of the SME. Question 1 captured the years of experience and duty title of the SMEs. The years of experience ranged from 3 years to 34 years with an average of 8.5 years of experience. The duty titles included Lead Engineers and EW Branch Chiefs of various USAF platforms. The average years of experience in fields of EW of all nine subjects that responded, prove they are SMEs in MD.

Question 2 asked "Does the provided Mission Data database properly represent an operational database by using hypothetical threat parametrics?". Out of the nine SMEs; one Strongly Agreed, four Agreed and four were Neutral. Assigning a value of 1 to 5 for

Strongly Disagree to Strongly Agree respectively, there is an average of 3.66 or a rating of slightly under Agree.

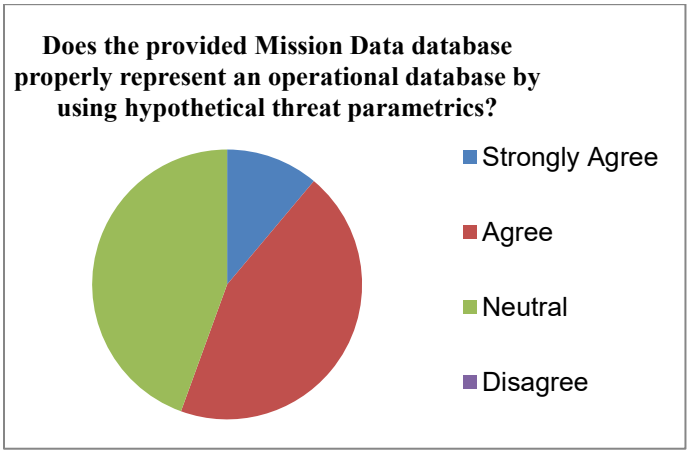


Figure 12. Question 2 Results

Question 3 asked "Does the provided Mission Data database use enough types of parametrics (frequency, pulse width, pulse repetition interval, etc) to identify a threat or type of threat? If not, please use the space provided to include additional parameters". Out of the nine SMEs; five Agreed, three were Neutral and one Disagreed. Similarly to Question 2, there is an average of 3.44 or a rating of slightly above Neutral.

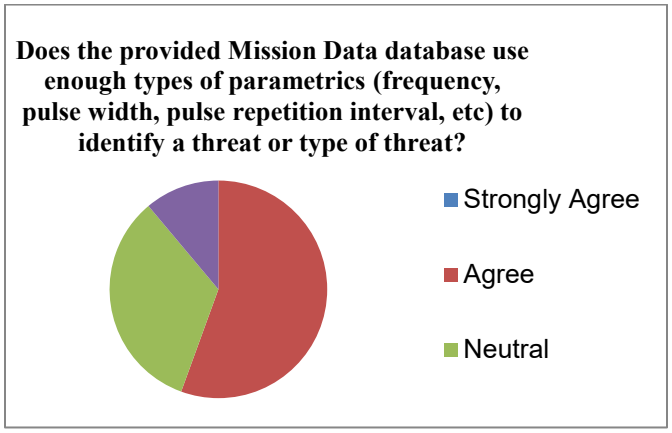


Figure 13. Question 3 Results

Questions 1 through 3 were designed to assess the validity of the test database. The success criteria for both questions needing a rating of Agree was slightly lower on average. However, the SMEs provided notes and additional details for their assessments in the questionnaire. The most common reasoning provided by the SME was that the dataset was not as complex as an operational dataset. This was an expected observation as described in the limitations and assumptions of this research. The provided dataset was created with unclassified data and attempting to create a dataset with certain types of parameters could result in a security violation by association. The second most common comment was a lack of representation of more parameters. This was also expected as this research was meant to prove the concept of RStudio processing with limited radar parameters. Additional parameters would certainly refine the identification but are not required. Chapter I provided insight on security classification limitations for this research. Maintaining an unclassified document relied on using public and unclassified Surface-to-Air radar parameter guidance to remove possible associations to operational radar parameters. Chapter V provides steps on how to proceed with future research using this method, recommending for both an increase in parameter complexity and classified parametric data.

Question 4 asked the SMEs to give a rating of importance of each of the provided parameters. The average of each parameter was then calculated and displayed in Figure 14. From the results, Frequency and PRI are both considered the most important with a perfect rating of 5, closely followed by Pulse Width at 4.44 and Scan Rate at 3.66. Power on average is considered low importance and would be recommended for future

development in machine learning mission data to be removed or weighted lower. This question did not have a success criteria and provides additional findings.

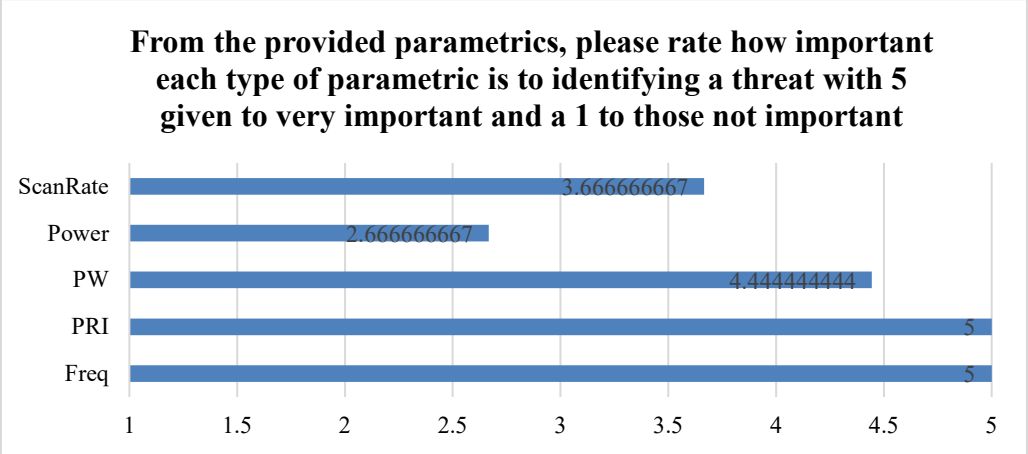


Figure 14. Question 4 Results

Identification Comparison

Question 5 aimed to determine the accuracy of the SME answers compared to the correct answers. It asks the SMEs to categorize a series of twenty-five new sets of parametrics not found in the original dataset by using the test dataset as reference. The SMEs identified all twenty-five parameter sets correctly, with the exception of a four which will be analyzed in this section. Table 1 below shows a confusion matrix, similarly to the RStudio output.

	SA-X Search	SA-X Track	SA-X Guide	SA-Y Search	SA-Y Track	SA-Y Guide	AI-X Track	AI-X Guide	AI-Y Track	AI-Y Guide	Unknown
SA-X Search	18	0	0	0	0	0	0	0	0	0	0
SA-X Track	0	11	0	0	0	0	0	0	0	0	0
SA-X Guide	0	0	12	0	0	0	0	0	0	0	0
SA-Y Search	0	0	0	15	0	0	0	0	0	0	0
SA-Y Track	0	0	0	1	12	0	0	0	0	0	0
SA-Y Guide	0	0	0	0	0	18	0	0	0	0	0
AI-X Track	0	0	0	0	0	0	18	0	0	0	0
AI-X Guide	0	0	0	0	0	0	0	12	0	0	0
AI-Y Track	0	0	0	0	0	0	0	0	18	0	0
AI-Y Guide	0	0	0	0	0	0	0	0	0	12	0
Unknown	0	1	0	2	0	0	0	0	0	0	0

Table 1. Question 5 Results

The matrix displays the SME answers in comparison to the correct answers. Each column shows the corresponding possibilities determined by the SME identifications. All threats were properly identified by the SMEs with the exception of four cases. These cases were identified as Unknown or misidentified. All four of the sets were examples of unknown sets as described in Chapter III. Unknown sets were those which belonged to one of the threats in the dataset with one slightly altered parameter to simulate an unknown parameter set of the threats. Analyzing the confidence levels of all twenty-five

parameter sets, gives us another view of how strongly the SMEs felt about each of their answers and more specifically, how they felt about the unknown sets.

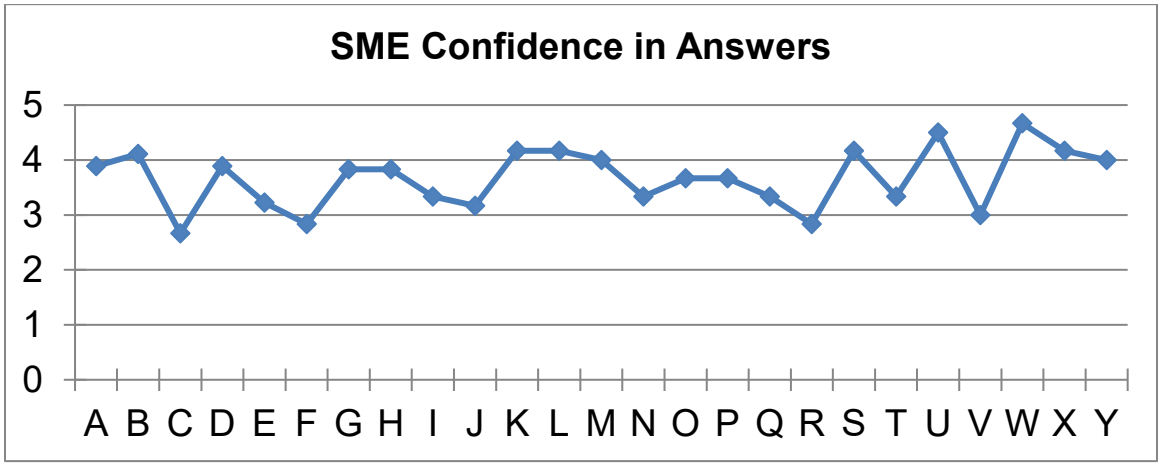


Figure 15. Question 5 Confidence

Analyzing the confidence levels, we see that the overall confidence in Answer C and R were lower than most of the other parameter sets. These two parameter sets were both examples where one or more of the parameters did not belong to any of the threats or belonged to threat with conflicting parameters. For example, parameter set R has a correct answer of SA-Y Search and four of the determining parameters support that answer. However, the Frequency was slightly lower than what the dataset represented and corresponded to SA-Y Track. One SME chose SA-Y Track while the remaining opted for SA-Y Search with overall low confidence to reflect the frequency variation. Answer P was also wrongly identified as Unknown but in this case the confidence is high as the SMEs were confident on the answer being Unknown rather than misidentify.

The SME accuracy from all twenty-five parameter sets gathered from Table 1 gives us an overall accuracy of 97.3%. Comparing this result to the RStudio KNN accuracy found in Chapter III of 92%, we see that the KNN algorithm was only 5.3% less

accurate compared to the SMEs at identifying EW threats. The goal of this research was to present evidence that a machine learning data processing tool could identify threats as close as SMEs to assist in the MD production process. These results prove that it is possible to use machine learning to assist in MD reprogramming.

Summary

The SME questionnaire was used to validate the test dataset. The validation results highlighted that the SMEs believe this type of dataset would benefit from having more complex threat parameters (similar to operational MD datasets). This supports the conclusion that additional research employing actual threat data to create a more robust dataset is warranted. Twenty-five new parameter sets were provided to be identified and these were identified with a 97.3% accuracy. Comparing this result to the 92% from KNN, the accuracy of the machine learning tool is similar to that of the SMEs.

V. Conclusions and Recommendations

Chapter Overview

This research provides evidence that using the RStudio KNN algorithm would aid SMEs in the task of reprogramming MD. This concept could be further refined in the proper secure environment and with the assistance of additional reprogramming center support. Attempting the KNN identification method using a classified dataset with allow for more accurate representation of current threat radars. The support of the 53EWG will allow access to classified networks, to include MD databases and any reprogramming tools that require clearance to properly analyze. Considering reprogramming is an iterative process, any systems that reduce SME workload would result in an expedited fielding of software for all supported platforms.

Conclusions of Research

The most relevant finding from this research is that the RStudio KNN categorization accuracy percentage was very similar to SME identification accuracy. The SME accuracy of the new parameter set was 97.3% while KNN categorization accuracy was 92%. A difference of only 5.3% proves that a machine learning algorithm is comparable to SME results using the same dataset. Using SME feedback, a more robust dataset with actual classified data would help test this data processing tool further for operational use. The importance of parameters varied depending on SME feedback. Frequency and PRI were the higher priority determining parameters to the engineers, while power was not valued as highly. Using a classified representative dataset with operational threat parametrics, the SME can adjust the KNN value given to each

parameter. Depending on the SME, the weighting values for each parameter will vary and provide additional control to the SME in identifying based on their preference.

AFI 10-703 provided the phases of reprogramming along with the expected products from the 53EWG [1]. During the Determine Impact phase, a SME using the KNN categorization for new threat parametric data for a reprogramming request, can use the machine learning KNN categorization to quickly generate the impact on the fielded MD. The System Impact Message deliverable of this phase would reach deployed aircrews faster than waiting for the SME to assess the impact. During the Reprogram phase, a SME can utilize the KNN categorization used to assess the impact then reevaluate threat prioritization to determine what to display the aircrews. If not change is required, the SME can begin regression testing to verify previous MD was not negatively affected by adding new threat parametric data.

Significance of Research

This research was meant to provide proof that an existing data processing tool such as RStudio using a machine learning KNN algorithm could be used to solve the issue of needing rapid MD production. The categorization provided by this tool could be used to expedite this process. SMEs could choose to run the algorithm in a fully operational dataset once this method is tested with classified data in order to identify a majority of threats allowing the SMEs to simply verify the results, thus saving a considerable amount of time. After a verification process, the MD file would be one step closer to completion.

Recommendations for Action

AFIT and the research team should engage with the 53EWG and provide the findings of this thesis. This would support the potential of using machine learning in operational MD production. This evidence would allow the support from the organization to pursue follow up research using the RStudio KNN method and facilitate using classified datasets to verify this process using actual threat parameters.

Recommendations for Future Research

This research used a simple dataset to prove this concept and the intent was to use a relevant dataset to test the KNN algorithm. However, this is a fact stated by many of the SME throughout their responses. The dataset should be more complex to be at a similar standard to actual MD reprogramming datasets used by the 53EWG SME. We ensured that the dataset would remain unclassified and hypothetical by utilizing public FAA Surface-to-Air radar parameter guidance to remove the potential of this research becoming classified. However, creating a classified dataset using actual radar parametrics would bolster this method of reprogramming for operational use. The concept of using RStudio KNN algorithm was proven by this research to replicate identification accuracy of SMEs to assist in MD reprogramming. Using a more complex operational and classified dataset would be the next step for a future thesis.

Appendix

Appendix A

Subject Matter Expert Mission Data Questionnaire

Background information

This information will enable the Air Force Institute of Technology to contact you if there are any questions about the data. The data will be used to support mission data production research and all questions below are tailored to assess the results of the research using your feedback. A copy of this questionnaire will be send via e-mail. Please return the questionnaire at your earliest convenience.

1. Please provide the following information.

Name:

Duty Title:

Years of Experience:

2. Does the provided Mission Data database properly represent an operational database by using hypothetical threat parametrics?

Strongly Agree Agree Neutral Disagree Strongly Disagree

3. Does the provided Mission Data database use enough types of parametrics (frequency, pulse width, pulse repetition interval, etc) to identify a threat or type of threat? If not, please use the space provided to include additional parameters.

Strongly Agree Agree Neutral Disagree Strongly Disagree

Additional Parameters Needed:_____

4. From the provided parametrics, please rate how important each type of parametric is to identifying a threat with 5 given to very important and a 1 to those not important.

a. Frequency: 1 2 3 4 5

b. Pulse Repetition Interval: 1 2 3 4 5

c. Pulse Width: 1 2 3 4 5

d. Power: 1 2 3 4 5

e. Scan Rate: 1 2 3 4 5

5. Using the provided Mission Data database, please identify the following threats and rate your confidence on each answer with a 5 for very confident and a 1 for not confident.

a. Frequency: 7777 PRI: 190 PW: 12 Power: 90 Scan: 3

Answer:_____

Answer Confidence: 1 2 3 4 5

b. Frequency: 14444 PRI: 7 PW: 2 Power: 85 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

c. Frequency: 7935 PRI: 324 PW: 15 Power: 90 Scan: 6

Answer:_____

Answer Confidence: 1 2 3 4 5

d. Frequency: 3333 PRI: 158 PW: 11 Power: 90 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

e. Frequency: 15800 PRI: 97 PW: 10 Power: 85 Scan: 20

Answer:_____

Answer Confidence: 1 2 3 4 5

f. Frequency: 9472 PRI: 4 PW: 3 Power: 75 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

g. Frequency: 9002 PRI: 11 PW: 3 Power: 70 Scan: 4

Answer:_____

Answer Confidence: 1 2 3 4 5

h. Frequency: 3904 PRI: 157 PW: 14 Power: 90 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

i. Frequency: 11111 PRI: 99 PW: 12 Power: 90 Scan: 14

Answer:_____

Answer Confidence: 1 2 3 4 5

j. Frequency: 10233 PRI: 176 PW: 15 Power: 85 Scan: 18

Answer:_____

Answer Confidence: 1 2 3 4 5

k. Frequency: 6782 PRI: 14 PW: 3 Power: 75 Scan: 2

Answer:_____

Answer Confidence: 1 2 3 4 5

l. Frequency: 6172 PRI: 18 PW: 2 Power: 75 Scan: 2

Answer:_____

Answer Confidence: 1 2 3 4 5

m. Frequency: 8192 PRI: 11 PW: 4 Power: 70 Scan: 5

Answer:_____

Answer Confidence: 1 2 3 4 5

n. Frequency: 9723 PRI: 1 PW: 1 Power: 60 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

o. Frequency: 7129 PRI: 5 PW: 3 Power: 75 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

p. Frequency: 15983 PRI: 22 PW: 5 Power: 85 Scan: 5

Answer:_____

Answer Confidence: 1 2 3 4 5

q. Frequency: 14267 PRI: 7 PW: 2 Power: 85 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

r. Frequency: 13999 PRI: 85 PW: 9 Power: 85 Scan: 13

Answer:_____

Answer Confidence: 1 2 3 4 5

s. Frequency: 15783 PRI: 36 PW: 4 Power: 80 Scan: 6

Answer:_____

Answer Confidence: 1 2 3 4 5

t. Frequency: 8002 PRI: 11 PW: 3 Power: 70 Scan: 2

Answer:_____

Answer Confidence: 1 2 3 4 5

u. Frequency: 6908 PRI: 15 PW: 4 Power: 70 Scan: 4

Answer:_____

Answer Confidence: 1 2 3 4 5

v. Frequency: 15782 PRI: 99 PW: 9 Power: 85 Scan: 19

Answer:_____

Answer Confidence: 1 2 3 4 5

w. Frequency: 11725 PRI: 116 PW: 13 Power: 90 Scan: 11

Answer:_____

Answer Confidence: 1 2 3 4 5

x. Frequency: 7921 PRI: 3 PW: 3 Power: 75 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

y. Frequency: 15823 PRI: 7 PW: 2 Power: 85 Scan: 0

Answer:_____

Answer Confidence: 1 2 3 4 5

Bibliography

1. HQ USAF/A5R, “AIR FORCE INSTRUCTION 10-703 ELECTRONIC WARFARE (EW) INTEGRATED REPROGRAMMING ” 22 FEBRUARY 2017

2. C. Mellen. “Fire Controlman, Volume 2–Fire-Control Radar Fundamentals.” 2000. NAVAL EDUCATION AND TRAINING PROFESSIONAL DEVELOPMENT AND TECHNOLOGY CENTER

3. C. Wolff. Fire-control Radar or Tracking Radar. https://www.radartutorial.eu/02.basics/Fire-control%20radar.en.html

4. AN/ALR-56M Radar Warning Receiver (RWR). https://www.globalsecurity.org/military/systems/aircraft/systems/an-alr-56.htm

5. S. Kang et al., "Autonomously Deciding Countermeasures against Threats in Electronic Warfare Settings," 2009 International Conference on Complex, Intelligent and Software Intensive Systems, Fukuoka, 2009, pp. 177-184, doi: 10.1109/CISIS.2009.131.

6. D. Larose. “Data Mining and Predictive Analytics” 2015 Wiley. pp 463

7. Federal Aviation Administration. RADAR QUICK REFERENCE GUIDE. 23 July 2007. https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/safety_ops_support/spec_management/library/view/documents/Radar%20Quick%20Reference%20Guide.pdf

8. B. Zhang and W. Zhu, "Research on Decision-making System of Cognitive Jamming against Multifunctional Radar," 2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Dalian, China, 2019, pp. 1-6, doi: 10.1109/ICSPCC46631.2019.8960757.

9. S. Kuzdeba, A. Radlbeck and M. Anderson, "Performance Metrics for Cognitive Electronic Warfare - Electronic Support Measures," MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, 2018, pp. 1-9, doi: 10.1109/MILCOM.2018.8599698.

Form Approved
OMB No. 074-0188

REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
22-11-2021	Master's Thesis	November 2020 - November 2021

TITLE AND SUBTITLE

Machine Learning Application For Mission Data Reprogramming

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Bingham, Paolo A., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENV-MS-D-041

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
53rd Electronic Warfare Group
210 Ave. D Eglin AFB, FL
PHONE and 53EWGstaffworkflow@us.af.mil
ATTN: Mr. Dylan Duplechain, GS-15

10. SPONSOR/MONITOR'S ACRONYM(S)

53EWG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Before entering a conflict or theater, USAF aircraft require updated mission data software reprogramming. Mission data controls all electronic warfare (EW) operations of the aircraft. EW operations include identifying and jamming radar operated systems, whether they are friendly or hostile. The process of reprogramming software is continuous and routinely updated for every EW system annually. On specific circumstances, the process can be expedited to months, but this puts a strain on the development team and shifts all attention to one specific mission data file. Unfortunately, a growing number of requests to upgrade mission data to a higher priority state, has created a backlog in the reprogramming process. The result is that now many requests are delayed or simply rejected. Successful reprogramming requires a mission data developer first categorize the radar emitter. This process involves matching all radar signal parameters to a known signal. This research developed a method to use machine learning data processing to assist in the reprogramming of mission data. Using a mission data processing algorithm, this research demonstrated how the development team can acquire a precise identification of a radar emitter by allowing the categorization be performed by machine learning.

15. SUBJECT TERMS
Electronic Warfare, Mission Data, Machine Learning

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Brent T. Langhals, AFIT/ENY
U	U	U	UU	48 44	19b. TELEPHONE NUMBER *(Include area code)* (520) 400-3751 (brent.langhals@afit.edu)