ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Reverse Modeling and Autonomous Extrapolation of RF Threats

Sanguk Noh[1] and So Ryoung Park[2]

[1] School of Computer Science and Information Engineering, The Catholic University of Korea
Bucheon, 420-743, Republic of Korea
sunoh@catholic.ac.kr

[2] School of Information, Communications, and Electronics Engineering, The Catholic University of Korea
Bucheon, 420-743, Republic of Korea
srpark@catholic.ac.kr

Abstract

This paper addresses the investigation of the basic components of reverse modeling and autonomous extrapolation of radio frequency (RF) threats in electronic warfare settings. To design and test our system, we first model RF threats using the radioactive parameters received. The enemy radar simulated with a transponder or emitter transmits electronic signals; next, the sensors of the system intercept those signals as radioactive parameters. We generate the attributes of RF threats during communication between the electronic emissions of RF threats and the receivers of our system in various electronic warfare scenarios. We then utilize the data acquired through our system to reversely model RF threats. Our system carries out the reverse extrapolation process for the purpose of identifying and classifying threats by using profiles compiled through a series of machine learning algorithms, i.e., naive Bayesian classifier, decision tree, and k-means clustering algorithms. This compilation technique, which is based upon the inductive threat model, could be used to analyze and predict what a real-time threat is. We summarize empirical results that demonstrate our system capabilities of reversely modeling and autonomously extrapolating RF threats in simulated electronic warfare settings.

Keywords: *Autonomous reverse extrapolation of threats; Data Mining using machine learning algorithms; Modeling and generating attributes of threats; Simulated electronic warfare settings.*

1. Introduction

Despite of potential danger in electronic warfare (EW) environments, first of all, our agents need to reversely extrapolate and autonomously identify threats in order to ensure their continual functionality. This paper investigates the basic components of reverse modeling and autonomous extrapolation of radio frequency (RF) threats in simulated EW settings. Autonomous situation awareness includes that the sensors perceive the signals of a dynamically changing environment, and the agents accumulate the processed data into knowledge bases. The critical step is to make the use of a specific knowledge to predict what kinds of situation will happen in an imminent future. The agents can be equipped with tracing and recognizing the state of incessantly changing and urgent environments. It is not a simply uncalculated response to a given snapshot but an elevated intelligence to make the agents adaptively operate. Thus, autonomous situation awareness is an indispensable component for an agent to be rational in the process of formulate its adaptive knowledge. This function can be widely applied to various fields such as battleground situation, traffic situation, and any kind of disaster situation [1, 2, 3].

For the reverse modeling and extrapolation of RF threats, we are obliged to use the observed or estimated attributes in place of the real attributes. In electromagnetic transmission, the radiated signal from transmitter will be modified and distorted for several reasons, and then arrived at the receiver [4, 5, 6, 7, 8, 9]. The signal power will be modified by the atmospheric loss, antenna gains, hardware losses, weather condition, and so on. The signal frequency will be transformed by the relative velocity of the RF threat and receiver. Under multipath fading environment, the signal may spread with some delay spread factor. That is, the observed attributes at the receiver for the reverse modeling could be considerably different form the real attributes at the transmitter in RF threats. To generate the observed attributes for the reverse modeling and to estimate the real attributes from the observed one, we examine the modifying principle of the electromagnetic waves during transmission in battlefield scenarios.

Given observed attributes of RF threats sensored by our agents in electronic warfare settings, we suggest a reverse extrapolation mechanism of RF threats through machine learning algorithms, i.e., both supervised naive Bayesian classifier [10] inductive decision tree algorithm [11], and unsupervised k-means clustering algorithms [12]. For our agents to have a reverse model of RF threats in a specific situation, we endow them with a set of operational knowledge. The knowledge formulated is constructed by compiling threat systems and their attributes into the resulting outputs of three machine learning algorithms. The compiled knowledge accumulated offline can be obtained from both supervised and unsupervised machine

learning algorithms. In this paper, further, the performance of each compilation method is measured so as to compare its accuracy with the others. The various compilations provide our agents with a spectrum of approaches to extrapolating reverse models under dangerous situations in EW settings.

To differentiate the types of RF threats, for example, search radars, tracking radars, and missile guidance seekers, we abstract reverse models from several types of threats in the simulated EW settings using compilation techniques. Applying both supervised and unsupervised machine learning algorithms to finding regularities has been used to detect specific patterns in many domains [13, 14] but, to our best knowledge, it could be one of new attempts for the reverse extrapolation of RF threats in electronic warfare scenarios. In our framework, both of the supervised and unsupervised machine learning algorithms compile the example situations into an operational knowledge to be applicable for autonomous situation awareness. Our approach leads to reversely model RF threats, to recognize given situation at hand based upon the compiled model, to rapidly respond to the fatal condition, and, as a consequence, to enhance our agents' continual survival.

The following section addresses the representative attributes of RF threats and design our rational agents which are equipped with reverse models extrapolating RF threats. We further generate the attributes of RF threats that realistically simulate electronic warfare scenarios given any RF threat. Section 3 describes our agent's reverse extrapolation process of threat identification in detail. Section 4 evaluates our framework empirically, and analyzes the experimental results. In conclusion, we summarize our result and discuss further research issues.

2. Analyzing Reverse Models of RF Threats and Generating Attributes for Reverse Modeling

To reversely extrapolate threats given in electronic warfare settings, we first abstract features from various RF threats and then model RF threats using the radioactive parameters received. In this section, we formulate the electronic signals of the RF threats into possible parameters for their simulated reverse extrapolation and design the architecture of our agents being capable of processing the reverse extrapolation.

2.1 Reversely Modeling RF Threats and Designing Reverse Extrapolation Process

Since our agents are assumed to perceive a threatening situation only through their radar receivers in EW settings, the RF threats that they can detect are divided into search radar, tracking radar, and missile guidance seeker [15, 16]. The RF threats can be applied to land-based, shipborne, and airborne radar systems based on the platform. Before we implement all the platforms, as the first step, we will test our agents which can be operational on the land-based platform [5, 15].

The representative attributes for agents' reverse model of RF threats in EW settings are described in Table 1. The signals perceived by radar receivers are translated into a set of variables. Given the variables, the attributes that can characterize the threats should be picked up. The attributes in Table 1 are determined to effectively discriminate three threat types among all potential threats. As shown in Table 1, the attributes acquired from radar sensors are radar frequency, pulse width, pulse power, and pulse repetition interval (PRI). The second column of Table 1 presents their values in specific ranges, and the third column describes three threat types identified, i.e., search radar, tracking radar, and missile guidance seeker.

Table 1: Relevant attributes modeling RF threats and threat types

Attributes	***Ranges***	***Threat Types***
Radar Frequency	3MHz ~ 40GHz	Search Radar / Tracking Radar / Missile
Pulse Width	0.1 ~ 5 μs	
Pulse Power	1KW ~ 1MW	
Pulse Repetition Interval (PRI)	1 μs – 1 ms	

The final goal in this research is to design and develop autonomous agents that can reversely extrapolate RF threats represented by the above attributes in Table 1, while operating in simulated electronic warfare settings. The reverse extrapolation will be extended to the range that our agents can identify not only threat types but also their block diagrams. We plan to create the block diagram which presents a certain operational principle of each threat, such as track-while-scan (TWS) radar or continuous-wave (CW) radar. In this paper, the first step towards this end is to acquire the characteristic signals of threats, and to reversely extrapolate the threat systems. The enemy's radar system simulated with a transponder or emitter transmits electronic signals; next, the radar sensors of our agents receive those signals as radioactive parameters. Given raw data sensed, the preprocessing module of our system further extracts more radioactive

variables. We then reversely extrapolate the threats into one of search radar, tracking radar, and missile guidance seeker based upon categories compiled during off-line. The architecture of reverse extrapolation system is illustrated in Fig. 1.

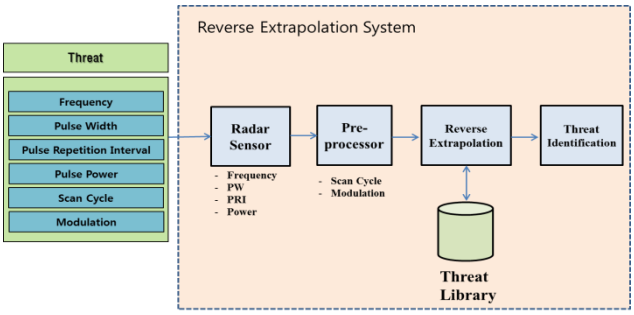

Fig. 1 The architecture of reverse extrapolation system

2.2 Generating Attributes for Reverse Modeling

To obtain the observed attributes of an RF threat at the receiver in electronic warfare settings, we examine the modifying principle of the electromagnetic waves during transmission and the estimating method of a real attribute from the modified one.

2.2.1 Modification of Signal Power

The most significant loss in power is the free-space path loss which is proportional to the square of the distance between the transmitter and receiver, and also proportional to the square of the frequency of the electromagnetic wave. In the far field where spherical spreading can be assumed, the free-space path loss L_{fs} can be expressed as [6]

$$L_{fs} = \left(\frac{4\pi f_0 R}{c}\right)^2, \qquad (1)$$

where f_0 is the frequency of RF signal, R is the distance between RF threat and receive, and c is the velocity of light. Other losses generated from various environments can be considered. The losses by atmospheric absorption due to oxygen L_{oxy} and water vapor L_{wv} are given by the Van Vleck equations [8, 9]. The loss due to rain L_{rain} increases with increased rainfall rate and radar frequency [4]. The losses L_{HW} generated by hardware (operator, collapsing, filter mismatch, and so on) may be considered if necessary [4].

Using one-way attenuation model, the received power P_r can be calculated from the transmitted power P_t by

$$P_r = \frac{P_t G_t G_r}{L_{total}} \qquad (2)$$

where $L_{total} = L_{fs} L_{oxy} L_{wv} L_{rain} L_{HW}$, G_t and G_r the transmitted and received antenna gain, respectively. After sensing the RF signal at the receiver, the received power and frequency can be observed. Then, we can estimate the transmitted power of RF signal as

$$\hat{P}_t = \frac{P_r \hat{L}_{total}}{G_r^2}. \qquad (3)$$

We assume that the transmitted antenna gain be equal to the received antenna gain and $\hat{L}_{total}$ is the calculated with the estimated distance and frequency considering the atmosphere and weather conditions.

The first row in Table 2 shows an example of the modification of RF signal power. When $P_t = 50$kW, $R = 30$km, $f_0 = 10$GHz, $G_t = G_r = 20$dB, and rainfall rate is 12.5mm/h, the received power is about 1.16W and the estimated power is about 450kW assuming that the estimated distance is 32km.

2.2.2 Modification of Signal Width

When a pulse is passed through a high-pass filter, the result is a positive spike at the leading edge and a negative spike at the trailing edge. By using the positive spike to start a counter and the negative spike to stop the count, it is possible to very accurately measure the pulse width [4]. However, under the multipath fading environment, the pulses from multipath do not arrive at the same time since the path lengths are different from each other. Then, a pulse will spread and consequently the pulse width will widen. In general, delay spread can be interpreted as the difference between the time of arrival of the earliest significant multipath component (typically, the line-of-sight component) and that of the latest components. Denoting the power delay profile of the multipath channel by $A_c(\rho)$, the mean delay of the channel is [7]

$$\bar{\rho} = \frac{\int_0^\infty \rho A_c(\rho) d\rho}{\int_0^\infty A_c(\rho) d\rho}, \qquad (4)$$

and the root mean square (rms) delay spread is given by

$$\rho_{rms} = \sqrt{\frac{\int_0^\infty (\rho - \bar{\rho})^2 A_c(\rho) d\rho}{\int_0^\infty A_c(\rho) d\rho}}. \qquad (5)$$

When a pulse with width τ is transmitted through the multipath fading channel with rms delay spread ρ_{rms}, the

observed pulse width at the receiver can be expressed as $\hat{\tau} = \tau + \rho_{rms}$. The second row in Table 2 shows an example of the modification of RF signal width. When $\tau = 0.5\,\mu s$ and $\rho_{rms} = 0.07\,\mu s$, the observed pulse width is about $0.57\mu s$. If the rms delay spread measures $0.05\mu s$, the pulse width will be estimated at $0.52\mu s$.

2.2.3 Modification of Signal Frequency

When the transmitter or receiver is moving, a change in frequency of electromagnetic waves, namely Doppler shift can be occurred. Generally, the observed frequency at the receiver f_r is given by [6]

$$f_r = \left(\frac{c + v_r}{c + v_t}\right) f_0 \approx \left(1 + \frac{\Delta v}{c}\right) f_0, \qquad (6)$$

where f_0 is the emitted frequency at RF threat, c is the velocity of light, v_r is the velocity of receiver, v_t is the velocity of RF threat, and Δv is the velocity of the receiver relative to RF threat. When the observed frequency at the receiver is f_r, the estimated frequency can be expressed as

$$\hat{f_0} = f_r / \left(1 + \frac{v_r}{c}\right), \qquad (7)$$

assuming that the velocity of RF threat is unknown and setting zero. The third row in Table 2 shows an example of the modification of RF signal frequency. When $R = 30$km, $f_0 = 10$GHz, $v_r = 290$m/s, and $v_t = 10$m/s, the observed frequency is to be nearly 10GHz.

Table 2: An example of attributes in the case of $\boldsymbol{R = 30}$km

Attributes	***Ranges***	***Threat Types***	***Estimated Values***
Radar Frequency	3MHz ~ 40GHz	Search Radar / Tracking Radar/ Missile	453kW
Pulse Width	0.1 ~ 5 μs		0.52 μs
Pulse Power	1KW ~ 1MW		10GHz

3. Reverse extrapolation of RF threats

To make our agents adaptable to simulated EW settings, we use machine learning algorithms, i.e., naive Bayesian classifier, inductive decision tree algorithm, and *k*-means clustering algorithm, and compile the example scenarios of RF threats into the resulting model of output.

As a supervised machine learning algorithm, in this section, we consider a naive Bayesian classifier and an inductive decision tree algorithm. A naive Bayesian classifier in simulated EW settings can be defined as follows: [2].

$$P(h_j \mid x_i) = \frac{P(x_i \mid h_j)P(h_j)}{\sum_{j=1}^{m} P(x_i \mid h_j)P(h_j)} \qquad (8)$$

where

- a set of attributes of an RF threat, $X = \{x_1, x_2, \ldots, x_n\}$;
- a set of types (or classes) of an RF threat, $H = \{h_1, h_2, \ldots, h_m\}$;
- $P(h_j|x_i)$ is the posterior probability of types of an RF threat h_j, $h_j \in H$, given that x_i, $x_i \in X$, is an observable attribute of an RF threat.

In our electronic warfare environments, the set of attributes of an RF threat, *X*, includes those described in Table 1, and the set of types of an RF threat is composed of search radar, tracking radar, and missile guidance seeker. Given a set of training data in this domain, Bayes theorem allows our agents to assign the posterior probabilities of types of an RF threat, $P(h_j|x_i)$. Our agents calculate $P(h_j|x_i)$ during online, and determine the specific type of an RF threat as the probability of a specific threat is greater than those of the others.

The decision tree approach such as ID3, C4.5 [11] and CN2 [17] uses a strategy of divide-and-conquer, which partitions the whole domain space into several types of an RF threat $C = \{c_1, c_2, \ldots, c_m\}$. From other point of view, the inductive decision tree algorithm is to find out a set of ordered attributes of an RF threat, $X = \{x_1, x_2, \ldots, x_n\}$, which separates the RF threats into a correct model with the highest information gain first. A decision tree has internal nodes labeled with attributes of an RF threat $x_i \in X$, arcs associated with their parent attributes, and leaf nodes corresponding to a set of types of an RF threat $c_j \in C$. We thus generate a decision tree representing the reverse model of various RF threats to our agents in the simulated EW setting. Based upon the generated tree, the output model can be obtained and used to interpret a new threat environment for the purpose of deciding whether any potential threat is encountered or not.

As an unsupervised machine learning algorithm, we also consider a k-means clustering algorithm [12] that aims at converging to a local optimum in an iterative refinement fashion. Given a set of instances or examples, $\{y_1, y_2, \ldots, y_n\}$, where an instance is a m-dimensional vector of attributes, the algorithm is to partition *n* instances into the *k* sets of $S=\{S_1, S_2, \ldots, S_k\}$ so as to minimize *V* in the following equation (9)

$$V = \sum_{i=1}^{k} \sum_{j \in S_i} |y_j - \mu_i|^2 \quad (9)$$

where μ_i is the mean of instances in S_i.

To measure the distance between two instances in the k-means clustering framework, we deploy two metrics, i.e., Euclidean distance and cosine similarity. The Euclidean distance from *a* to *b* is given by

$$d(a,b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots + (a_m - b_m)^2}, \quad (10)$$

where $a=(a_1, a_2, \ldots, a_m)$ and $b=(b_1, b_2, \ldots, b_m)$ are two instances in Euclidean m-space. In a similar way, the distance between two instances $a=(a_1, a_2, \ldots, a_m)$ and $b=(b_1, b_2, \ldots, b_m)$ using cosine similarity is given by

$$d(a,b) = \frac{a \cdot b}{\|a\| \cdot \|b\|} = \frac{\sum_{i=1}^{m} a_i \times b_i}{\sqrt{\sum_{i=1}^{m} a_i^2} \times \sqrt{\sum_{i=1}^{m} b_i^2}}. \quad (11)$$

We thus utilize both supervised and unsupervised machine learning algorithms mentioned above to inspire our agents with a reverse model of RF threats. Our agents equipped with the resulting models generated during offline are able to reactively cope with online situation. Given an electronic warfare state, our agents apply the best reverse model among compiled models to the state, and then realize what type of RF threats is given. In this line of approach [2], the offline computation for a set of compilation significantly reduce the response time and provide our agents with more chance to survive while having more time to react.

4. Experimental Result

To evaluate the performance of reverse extrapolation process for threat identification, we generate the simulation data using discrete uniform distribution and test the compiled models by applying them to simulated electronic warfare (EW) settings. For this experiment, we use WEKA (Waikato Environment for Knowledge Analysis) [18] for supervised machine learning algorithms, i.e., naive Bayesian classifier and decision tree algorithm, and implement k-means clustering algorithms as an unsupervised technique using Euclidean distance and cosine similarity metrics, respectively. We measure the performance of our agents with reverse models in terms of the correct identification of RF threats.

4.1 Compiled Models of RF Threats

In our experiment, we applied the theoretical background of Section 2 to our simulated EW settings for the generation of attribute values. For supervised machine learning algorithms, the training data consisted of a set of attributes, i.e., radar frequency, pulse width, pulse power, and pulse repetition interval (PRI), and a class, i.e., search radar, tracking radar, and missile guidance seeker, as specified in Table 1. For unsupervised machine learning algorithms, the training data were composed of only a set of attributes without an assigned class. In our experiment, the number of total instances for training was 3, 000.

To endow our agent with three reverse models of threat data, then, the threats as training data were compiled into a set of outputs, i.e., a statistical model, an inductive rule, and a number of clusters. For the naive Bayesian classifier, the resulting output was presented as a statistical model specifying the probability of occurrence of each attribute value given a class of RF threats. C4.5 as a decision tree algorithm presented its output as a set of reactive rules. The trained result of k-means clustering algorithm was a distribution of clusters mapping from the attributes of threats to the types of RF threats.

An example of statistical model compiled through the naive Bayesian classifier was described in Table 3. Since all of attributes were numerical or continuous, in our domain, its compiled output model was the mean and the variance of attribute values. We then calculated the probability distribution of the output values given a class using normal Gaussian distribution.

Table 3: An example of statistical model compiled through naïve Bayesian classifier

Attributes	***Classes***		
	Search Radar	***Tracking Radar***	***Missile***
Radar Frequency (GHz)	1.92 ± 1.14	6.07 ± 1.18	23.56 ± 9.51
Pulse Width (μs)	3.23 ± 1.04	1.16 ± 0.21	0.45 ± 0.19
PRI (μs)	504.50 ± 307.67	3.53 ± 0.79	2.05± 0.56
Pulse Power (KW)	280.32 ± 126.98	55.89 ± 25.98	26.51 ± 13.91

The output model of reactive rules compiled by C4.5 was described in Table 4. Based on the resulting model of a decision tree, one of compiled rules was "if (pulse_width > 0.79) and (pulse_width ≤ 1.50), then tracking_radar."

Table 4: An example of rules compiled through C4.5 decision tree

Classes	***Rules***
Search Radar	**if** (Pulse_Width > 0.79) **and if** (Pulse_Width > 1.50), **then** search_radar.
Tracking Radar	**if** (Pulse_Width > 0.79) **and if** (Pulse_Width ≤ 1.50), **then** tracking_radar.
Missile	**if** (Pulse_Width ≤ 0.79), **then** missile.

Table 5 and Table 6 indicated the outputs compiled by k-means clustering algorithm using the metrics of Euclidean distance and cosine similarity, respectively. The attributes values were normalized from 0 to 100 and, from each attribute perspective, the resulting values denoted the centers for each cluster, which referred to the means nearest to a prototype of the cluster. For example, in Table 5, the 933 instances of 'search radar' belonged to the cluster 1, and the 67 instances of the same class belonged to the cluster 2. Since the cluster 1 consisted of only 'search radar,' thus, the cluster 1 should be classified into the class of 'search radar' as a result. For autonomous situation awareness, the three resulting models of RF threats could widely be used in various EW situations.

Table 5: An example of cluster compiled through K-means clustering algorithm using Euclidean distance metric

Attributes	***Clusters***		
	Cluster 1	***Cluster 2***	***Cluster 3***
Radar Frequency (GHz)	4.87	71.13	17.94
Pulse Width (μs)	66.92	6.95	19.33
PRI (μs)	53.29	0.10	1.06
Pulse Power (KW)	57.46	4.99	10.33
Attributes	***Clusters***		
	Cluster 1	***Cluster 2***	***Cluster 3***
Search Radar	***933***	67	0
Tracking Radar	0	***1000***	0
Missile	0	300	***700***

Table 6: An example of cluster compiled through K-means clustering algorithm using Cosine similarity metric

Attributes	***Clusters***		
	Cluster 1	***Cluster 2***	***Cluster 3***
Radar Frequency (GHz)	4.81	59.03	13.53
Pulse Width (μs)	63.16	7.11	29.23
PRI (μs)	58.68	0.10	2.08
Pulse Power (KW)	56.94	4.87	13.32
Attributes	***Clusters***		
	Cluster 1	***Cluster 2***	***Cluster 3***
Search Radar	***830***	0	170
Tracking Radar	0	1	***999***
Missile	0	***999***	1

4.2 Performance of Compiled Models

First, we need to find a meaningful size of the training set which could guarantee the soundness of the learning hypothesis compiled by supervised machine learning algorithms including naive Bayesian classifier and C4.5 decision tree algorithm. We set up a bunch of training examples using discrete uniform distributions starting with 180 instances. In this learning curve, we found that the sufficient number of training instances was 480, as circled in Fig. 2. The learning curves show the resulting performances (%) vs. the sizes of training examples for three RF threat types, as depicted in Fig. 2.

The naive Bayesian classifier quickly acquired the reverse extrapolation process of RF threats, as shown in Fig. 2. Its best performance turned out 100% of correctness, while those of C4.5 decision tree algorithm did 99.60%, which was almost same as the best performance. In our simulated EW settings, the performance obtained by naive Bayes classifier was a little better than that of C4.5 decision tree algorithm

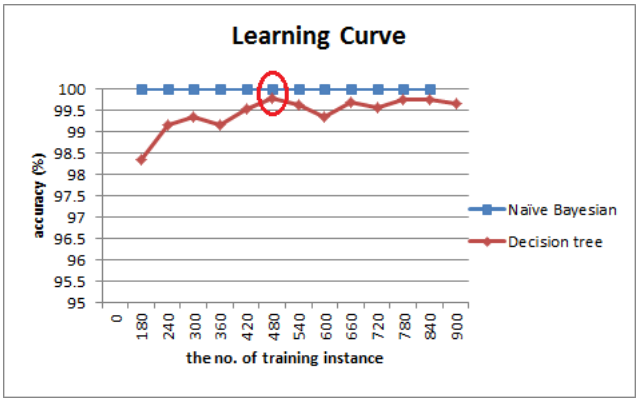

Fig. 2 The resulting performances (%) vs. the training data size for three RF threat types.

The output models compiled using supervised learning algorithms were tested by newly generated ten sets of 480 instances, which was optimally determined in Fig. 2. We could obtain the performances of the reverse extrapolation methods, as described in Table 7. Regarding the performance of the *k*-means clustering algorithm as a unsupervised learning technique, the ten sets of 3,000 instances divided into three (= *k*) classes of 1,000 ones were generated with three different initial centroids (means).

Table 7: Performances of compilation methods

Compilation Methods		***Performances***
Naïve Bayes		99.92 ± 0.11
C4.5		99.60 ± 0.11
ANOVA		$f = 46.75$
Compilation Methods	***Distance Metric***	***Performances***
K-means Clustering	Euclidean Distance	85.63 ± 2.27
	Cosine Similarity	93.50 ± 0.53
ANOVA		$f = 114.22$

We analyze the performance results in Table 7 using the standard analysis of variance (ANOVA) method. Since the computed values of $f = 46.75$ and $f = 114.22$ in ANOVA exceed 8.29 (= f .01,1,18) from the F distribution, respectively, we know that the performance of our agents, controlled by naive Bayesian classifier and C4.5 decision tree algorithm, shows meaningful difference in EW situations. In other words, the difference in their performance is not due to chance with probability of 0.99. Likewise, the performance between Euclidean distance and cosine similarity metric in case of k-means clustering algorithm reveals the same result with the above. In Table 7, the average performance of our agent using the naive Bayesian classifier in a simulated EW situation is slightly better than that of C4.5, while the agent using k-means clustering algorithm with cosine similarity metric outperforms the other agents with Euclidean distance metric.

4.3 Implementation of Test Programs

For a reverse extrapolation system equipped with outputs compiled through three machine learning algorithms, we separately implemented test programs using C# programming language. The reverse extrapolation of RF threats using naive Bayesian classifier is depicted in Fig. 3. To test the compiled knowledge, users input radioactive parameters for each attribute of RF threats at the left side of Fig. 3, select a specific algorithm, and then press the 'execute' button. The result of extrapolation is displayed at the bottom of left side, and the output panel, that is, the right side of Fig. 3 shows a statistical model and the result of threat identification given specific input parameters, as highlighted in red color.

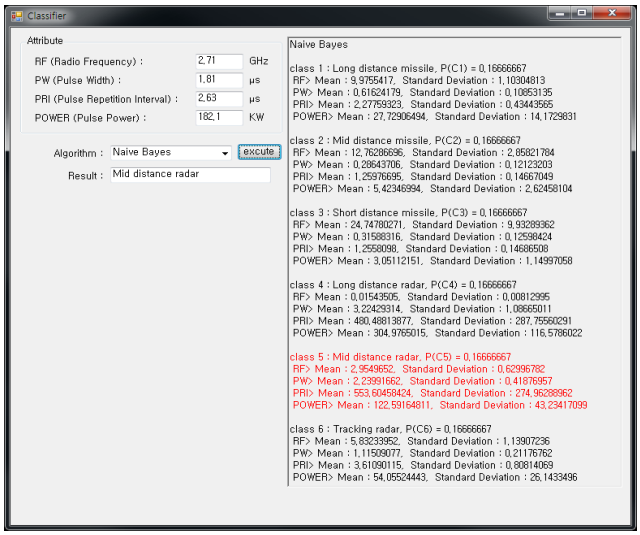

Fig. 3 The resulting reverse extrapolation using naïve Bayesian classifier.

Similarly, Fig. 4 and Fig. 5 show the reverse extrapolation using C4.5 inductive decision tree algorithm in the forms of tree diagram and text mode, respectively. The reverse extrapolation using k-means clustering algorithm, as depicted in Fig. 6, consists of four vertical axes representing four attributes, i.e., radio frequency, pulse width, pulse repetition interval (PRI), and pulse power, six horizontal lines for six classes in detail, and one resulting horizontal line as an output class. In Fig. 6, another

horizontal line of violet color comes up on the screen indicating that the resulting extrapolation class is 'an early warning search radar.'

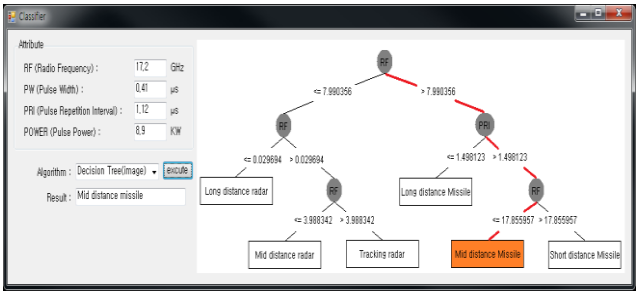

Fig. 4 The resulting reverse extrapolation using C4.5 decision tree diagram.

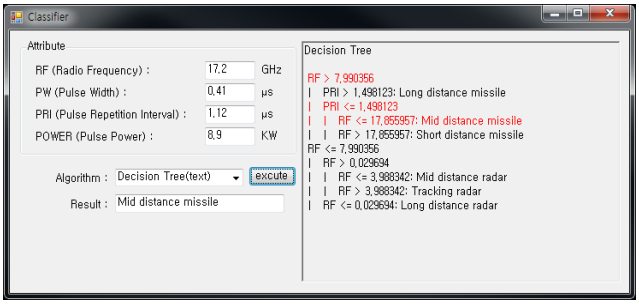

Fig. 5 The resulting reverse extrapolation using C4.5 decision tree in text mode.

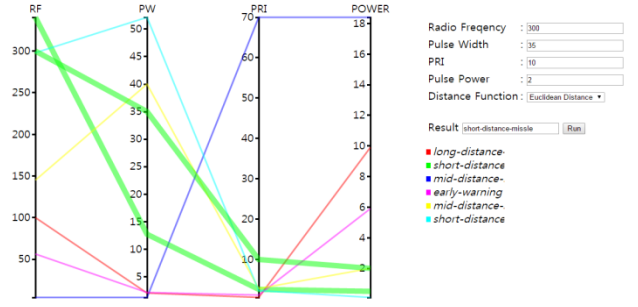

Fig. 6 The resulting reverse extrapolation using K-means clustering algorithm.

5. Conclusion and Future Work

It is indispensable for our agents to be equipped with capabilities of detecting threat signals, analyzing an electromagnetic environment, and providing a fast precise assessment of RF threats in simulated EW settings. In this paper, we showed a fully autonomous agent that reversely extrapolates various types of RF threats by using compilation techniques. For the reverse extrapolation process of RF threats, the threats were analyzed into a set of attributes, and the observed attributes were perceived at the receiver by using the modifying principle of the electromagnetic waves during transmission. The simulated threat data through uniform distributions were generated within the range of attribute values, and were compiled into a set of output to endow our agents with the reverse models of RF threats. Our agent's performance in the experiment proved that the agent's knowledge accumulated by compilation techniques was essential to threat identification and early warning, and to its continual survival in EW environments.

The final goal of this research is to repeatedly simulate various EW situations and for our agents to accurately identify the threat itself and its block diagram as well. In future work, we are implementing an integrated reverse extrapolation simulator, which consists of a module of communication between the transmitter of threats and the receiver of our agents for the generation of realistic attributes, a module of the block diagram presenting a certain operational principle of each threat, and a module of jamming techniques to test whether or not the identification of the threat is correct. We hope to be able to implement a fully autonomous agent to successfully identify RF threats as quickly as possible through our future work.

Acknowledgments

This work has been supported by the Electronic Warfare Research Center, Republic of Korea, under Grant EW41 "Reverse Extrapolation of RF Threats in Electronic Warfare Settings," 2013. We would like to thank our students, Jisu Ha and Cheolpyo Kim, for their help in implementing the machine learning algorithms.

References

[1] D.J. Bryant, F.M.J. Lichacz, J.G. Hollands and J.V. Baranski, Modeling situation awareness in an organizational context: Military command and control, in A cognitive approach to situation awareness: theory and application, eds. S. Banbury and S. Tremblay, Burlington, VT: Ashgate Publishing Company, Chapter 6. 2004.

[2] S. Noh and U. Jeong, “Intelligent Command and Control Agent in Electronic Warfare Settings”, International Journal of Intelligent Systems. Vol. 25, No. 6, 2010, pp. 514-528.

[3] J. Patrick and N. James, A Task-Oriented Perspective of Situation Awareness, in A cognitive approach to situation awareness: theory and application, eds. S. Banbury and S. Tremblay, Burlington, VT: Ashgate Publishing Company, Chapter 4, 2004.

[4] D.L. Adamy, EW 101: A First Course in Electronic Warfare, Artech House Publishers, Chapter 5. 2001, August 28, 2015

15:58 WSPC/ws-ijitdm ITDM20150828

[5] A. Golden Jr., Radar Electronic Warfare, AIAA Education Series, Chapter 2, 1988.

[6] B.R. Mahafza, Radar Systems Analysis and Design Using MATLAB, 3rd edition, CRC Press, Chapter 8, 2013

[7] M. Patzold, Mobile Fading Channels, John Wiley and Sons, Chapter 7, 2002.

[8] J.H. Van Vleck, "The absorption of microwaves by oxygen", Physical Review, Vol. 71, p. 413, 1947.

[9] J.H. Van Vleck, "The absorption of microwaves by uncondensed water vapor", Physical Review, Vol. 71, p. 425, 1947

[10] R. Hanson, J. Stutz and P. Cheeseman, Bayesian Classification Theory, Technical Report FIA-90-12-7-01, NASA Ames Research Center, AI Branch, 1991.

[11] J.R. Quinlan, C4.5: Programs for Machine Learning, Morgan Kaufmann Publishers, 1993.

[12] S.P. Lloyd, "Least squares quantization in PCM", IEEE Transactions on Information Theory, Vol. 28, No. 2, 1982, pp. 129-137.

[13] Q. Yang and X. Wu, "10 Challenging Problems in Data Mining Research", International Journal of Information Technology and Decision Making, Vol. 5, No. 4, 2006, pp. 597-604.

[14] L. Hamilton, Six Novel Machine Learning Applications, Forbes (2014), http://www.forbes.com/sites/85broads/2014/01/06/six-novel-machine-learning-applications/.

[15] A.E. Spezio, "Electronic warfare systems", IEEE Transactions on Microwave Theory and Techniques, Vol. 50, No. 3, 2002, pp. 633-644.

[16] J. Heikell, Electronic warfare self-protection of battlefield helicopters: A holistic view, doctoral dissertation Helsinki University of Technology, 2005.

[17] P. Clark and T. Niblett, "The CN2 Induction Algorithm," Machine Learning Journal, Vol. 3, No. 4, 1989, pp. 261-283.

[18] I.H. Witten, E. Frank and M.A. Hall, Data Mining: Practical machine learning tools and techniques, 3rd edition. Morgan Kaufmann Publishers, 2011.