I.J. Intelligent Systems and Applications, **2019, 7, 1-9**
Published Online July 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2019.07.01

Simulation for the Reverse Extrapolation of Radar Threats and their Verification

Sanguk Noh
School of Computer Science and Information Engineering, The Catholic University of Korea,
Bucheon 14662, Republic of Korea
Corresponding author E-mail: sunoh@catholic.ac.kr

So Ryoung Park
School of Information, Communications, and Electronics Engineering, The Catholic
University of Korea, Bucheon 14662, Republic of Korea
E-mail: srpark@catholic.ac.kr

Received: 11 January 2019; Revised: 20 February 2018; Accepted: 19 March 2019; Published: 08 July 2019

Abstract—Various and unpredictable electronic warfare situations drive the development of an integrated electronic warfare (EW) simulator that can perform electronic warfare modeling and simulation on radar threats. This paper introduces the basic components of simulation system that enables our agents to be operational in EW settings. In various simulation of EW environments, our agents can preset their path in the existence of enemy radars' surveillance and autonomously be aware of radar threats while they proceed in their own route. As reversely extrapolating radar threats given radio-active parameters received, our agents perform an appropriate jamming technique in order to deceive the enemy radar keeping track of our agents. Based upon the response of the radar threat attacked by the jamming techniques, our agents figure out the types of the radar threat and verify its identification. For the actual and helpful information, real radars with the probability of similarity could be prioritized from radar database. The integrated EW simulator that we have designed and developed in this paper enables our agents to perform such capabilities as reverse extrapolation of RF threats, its verification using jamming, and recommendation of similar radars, and to evaluate their autonomous behaviors in a tapestry of realistic scenarios.

Index Terms—Modeling and Simulation of Electronic Warfare, Machine Learning, Dempster-Shafer Theory, Intelligent Recommendation of Radars.

I. Introduction

Despite of potential danger in electronic warfare (EW) environments [1], first of all, our agents need to reversely extrapolate and autonomously identify the types of threats in order to ensure their continual functionality [2,3]. If our agents recognize a situation that a radar threat operates in the mode of searching, they should be ready to attack it. In progress of the enemy radar's tracking or missile attack, they should use jamming techniques to avoid its range of attack. To reversely extrapolate the types of radar threats, thus, we compile the attributes of threats into the possible models using machine learning algorithms [4]. Since there are several models for the types of radar threats according to a set of algorithms, a method is needed to determine a unique model from possible models. Towards this end, we investigate the method to integrate the reverse extrapolation models using Dempster-Shafer theory [5,6]. Our agents then can identify the unique type of radar threats given a set of models.

Given the response of radar threats attacked by a specific jamming and the comparison of parameter values received, this paper provides a method to recommend similar radar threats from radar database. To enhance their survivability in dynamic EW environments, the ultimate goal of our aircraft agents is to recognize the actual specification of the threat through their extrapolation to threats and verification process by jamming. Similarities of radars are defined by the attributes of parameters acquired by the receiver and by the degree of endurance to a jamming attack as well. We quantify the similarities into the difference between parameter values received and ones stored in database, and at the same time into the characteristic values denoting the effectiveness of jamming. The quantification of the similarity enables our aircraft agents to prioritize similar radars and to estimate one closest to what a realistic radar is.

In this paper, we analyze the components of a simulation system to reversely model the types of radar threats that emit electromagnetic signals based upon the parameters of the electronic information, and to verify the reverse extrapolation of radar threats using jamming techniques. We have designed and implemented the simulator, and have tested our intelligent agents' capabilities in various simulated EW settings. The simulator consists of the panels of radar threats, the electronic receiver detecting the threats, and the scenario display showing their interactions. The panel of a radar threat located on a territory includes the radar's view of a target, a set of its emitting parameters, two positions of a target jammed and a real target for reference, and a H/W block diagram of a radar. The panel of the electronic receiver which presents information for our aircraft agents includes the receiver's view of a radar threat, parameters received, types of a radar threat identified, a current jamming attack, and a list of radar recommended from radar database.

In the following section, we will describe our work while comparing it with related research. Section III explains how our aircraft agents with receiver decide the unique type of a radar threat and enumerate similar radars recommended from database, given the response of the radar. Section IV describes the architecture of a unit jamming simulator and an integrated EW simulator, respectively. Using the EW simulator, in section V, we validate our framework empirically, and present the experimental results. In conclusion, we summarize our results and discuss further research issues.

II. Related Work

To iteratively test and verify the capabilities of our friendly agents in EW environments, there have been a lot of researches on two theoretical backgrounds. From situation awareness perspectives, a group of researchers [2, 3, 7-9] emphasize on the agents' way how they formulize and model the situation they are encountering. These approaches analyze percepts obtained through sensors and formulate them into a specific model to successfully perform the agents' task. In our previous work [4], we provide a reverse extrapolation technique using compilation framework, which enables our agents to be fully aware of environments. In this paper, further, we integrate reverse models into a unique model by unifying several models compiled through different learning algorithms.

From the approaches for modeling and simulation in the field of simulated EW settings, they develop a kind of simulation system with only particular part of radar system, specific jamming technologies, or propagation characteristics [10, 11]. However, our current work in this paper follows the research on the modeling and simulation considering all the essential modules of EW, i.e., sending and receiving signals, range and angle tracking modules of radar threats, propagation modules of electromagnetic waves, jamming modules for electronic attacks, and so on. Further, our simulator provides additional critical capabilities, which are reversely estimating a hostile radar, uniquely determining the threat, and recommending a set of radars from database as a verification process. Our efforts towards this end will complete the fully autonomous agent from situation awareness to successful mission accomplishment in various EW situations.

III. Reverse Extrapolation of Radar Threats and Their Verification in EW Settings

This paper addresses a suite of methodology as follows; (1) how to provide the unique estimation of types of a radar threat, and (2) how to recommend a set of radars which are similar with the radar threat verified. We will start with the integration of multiple reverse models in simulated EW environments.

A. Integration of Multiple Reverse Models

Since our aircraft agents are assumed to perceive a threatening situation only through their radar receivers in EW settings, the RF threats on the land-based platform that they can detect are divided into search radar, tracking radar, and missile guidance seeker. 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 are determined to effectively discriminate three threat types among all potential threats. The attributes acquired from radar sensors are radar frequency, pulse width, pulse power, and pulse repetition interval (PRI). Given a set of attributes, three threat types are identified, i.e., search radar, tracking radar, and missile guidance seeker.

A set of radar instances is compiled into the individual model of RF threats. For our agents to have a reverse model of RF threats in a specific situation, we endow them with an operational knowledge. The knowledge formulated is constructed by compiling the attributes of threat systems into the resulting output of models. The compiled knowledge accumulated offline can be obtained from both supervised and unsupervised machine learning algorithms [4]. The various compilations provide our agents with a spectrum of approaches to extrapolating reverse models under dangerous situations in EW settings. In this paper, we expand our previous work to unify those models into the unique identification, which is the result integrated with reverse extrapolation models by the Dempster-Shafer method [5,6].

To formulate the decision of the type of RF threats from their possible reverse models, we apply the Dempster-Shafer theory to a set of results denoting the probability of types of a specific radar threat. Among the possible outputs of threat types, the combined prediction for our agents, α^{r_n}, is defined as follows:

$$\alpha^{r_n} = \frac{\alpha_i^{r_n} \times \alpha_j^{r_n}}{1-((1-\alpha_i^{r_n})\alpha_j^{r_n}+\alpha_i^{r_n}(1-\alpha_j^{r_n}))} \qquad (1)$$

where

- $\alpha_i^{r_n}$ and $\alpha_j^{r_n}$ are the confidence of the possible threat types r_n, obtained from revere extrapolation models *i* and *j*;
- r_n is an element of the set of search radar, tracking radar, and missile guidance seeker;

- $0 \leq \alpha_i^{r_n}$ and $\alpha_j^{r_n} \leq 1$;
- $\sum_n \alpha_i^{r_n} = 1$ and also $\sum_n \alpha_j^{r_n} = 1$.

The goal of aggregation is to combine outputs of reverse models when each of them estimates the probability of types of radar threats for our aircraft agents, and to produce a single probability distribution that summarizes various threat types. Using Dempster's rule, the resulting values of α^{r_n} indicate the degrees of agreement on different reverse models of reliability on the types of RF threats, but completely exclude the degrees of disagreement or conflict. The advantage of using the Dempster's rule for the integration of reverse models is that no priors and conditionals are needed.

Example. Let $\alpha_i^{r_n}$={0.75, 0.15, 0.10} and $\alpha_j^{r_n}$ ={0.80, 0.12, 0.08}, in case that a model *i* and a model *j* are used to reversely extrapolate the types of an RF threat monitored. Given two sets of probabilities, the combined estimation of a radar threat type using (1) can be computed as α^{r_n}={0.92, 0.02, 0.01}. Each resulting value for types of the radar threat is given

$$\frac{0.75 \times 0.80}{1-(0.75 \times 0.20 + 0.80 \times 0.25)} = 0.92$$

$$\frac{0.15 \times 0.12}{1-(0.15 \times 0.88 + 0.12 \times 0.85)} = 0.02$$

$$\frac{0.10 \times 0.08}{1-(0.10 \times 0.92 + 0.08 \times 0.90)} = 0.02$$

Normalizing the values of α^{r_n} ={0.92, 0.02, 0.01} emphasizes the combined estimation of the radar threat in a sense that the threat should be a search radar in the resulting form of {0.97, 0.02, 0.01}. The final normalized distribution on the types of the threat presents more clear identification, compared with two original distributions of {0.75, 0.15, 0.10} and {0.80, 0.12, 0.08}.

B. Recommendation of Similar Radars

To seek a realistic specification of an RF threat encountered, our aircraft agents compute the distance between the threat and a radar instance given database, and search for radar instances which are closest to the threat. The similarity of radars consists of the attributes of parameters acquired by the receiver and the degree of endurance to a jamming attack as well. These attributes are categorized into nominal or numeric values.

Depending upon whether or not the value of an attribute is discrete, each difference between an attribute value of an RF threat and that of a radar instance, δ^i, is differently taken into account. When the value of an attribute *i* is nominal, the difference can be attributed to the similarity as follows:

$$\delta^i = \begin{cases} 0 & if\ a_D^i = a_T^i \\ 1 & otherwise \end{cases} \tag{2}$$

where

- a_D^i is the value of an attribute *i* for a radar instance from radar database;
- a_T^i is the value of an attribute *i* for a specific threat.

In (2), δ^i will be 0 if two discrete values a_D^i and a_T^i are identical. Otherwise, it will be 1. When the value of an attribute *i* is numeric, the δ^i can also be contributed to the similarity as follows:

$$\delta^i = \frac{\sqrt{(a_D^i - a_T^i)^2}}{MAX(a_D^i) - MIN(a_D^i)} \tag{3}$$

where

- MAX(a_D^i) is the maximum value among continuous values of an attribute *i* for a radar instance from radar database;
- MIN(a_D^i)is the minimum value among continuous values of an attribute *i* for a radar instance from radar database.

The denominator in (3) normalizes the different range of various attribute values into the range of 0 and 1. Since we can calculate each distance between an attribute value of an RF threat and that of a radar instance regardless of the types of attribute value, we are now ready to represent a total distance between the RF threat and the instance from radar database.

The similarity between a specific threat and a radar instance, ω, then can be calculated as follows:

$$\omega = 1 - \frac{\sum_{i=1}^{n} \delta^i}{n} \tag{4}$$

where *n* is the number of attributes for a radar instance. In (4), if ω is closer to 1, the RF threat is much similar to the radar considered. Given a set of radar instances, the similarities for all of them are computed and closest radars to the specific threat are recommended.

IV. The Architecture of Simulators

We have designed and implemented the simulator for the reverse extrapolation of RF threats and their verification using jamming techniques. For the verification process of the identification of an RF threat in simulated EW settings, we have also developed a unit simulator and plugged it into the integrated simulator.

A. MATLAB Simulator

For verifying the performance of the proposed reverse extrapolation models in various and specific EW situations, we have used the EW simulations including the functional modules of radar threats, propagation, and electronic attacks, as shown in Fig. 1.

First, the identification is performed by the reverse extrapolation using the collected information for a specific radar threat under no jamming situation. Next, the appropriate jamming for the identified radar threat is selected and transmitted, and then, the radar signal influenced by jamming is received in aircraft. If the identification of the radar threat is correct, the selected jamming is effective to the radar threat, and as a result, the received signal and collected information from the radar threat change in the way intended by jammer. On the contrary, if the identification is incorrect, the collected information from the radar threat after jamming tends to be different from the way intended by jammer.

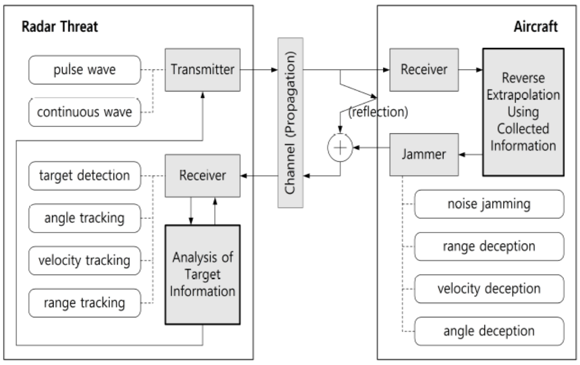


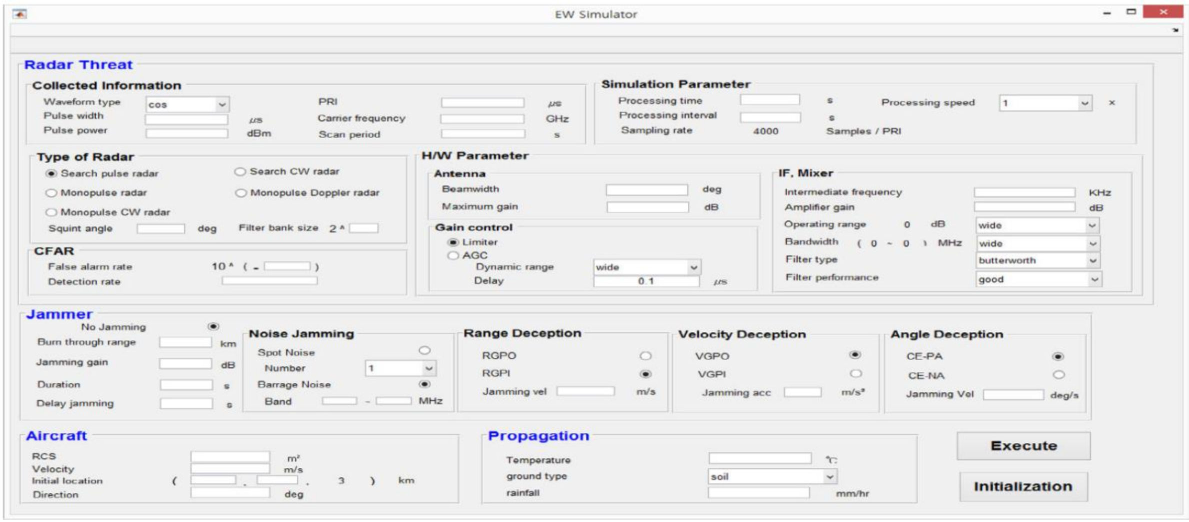
Fig.1. The block diagram of the verification system of reverse models using jamming techniques

We have implemented a unit simulator which has the essential elements of EW, such as detecting and tracking radar threats, jamming for electronic countermeasures or attacks, propagation of electromagnetic waves, and detailed battle scenarios. Fig. 2 shows the input screen of the implemented simulator using the software MATLAB ® 2017b.

The functional modules of radar threat including antenna, intermediate frequency (IF) conversion, automatic gain control (AGC), constant false alarm rate (CFAR) detection, range tracking with early/late gates, angle tracking using monopulse method, and velocity estimation with narrow-band filter banks have been considered for a realistic design with reference to the theoretical models or the principles of circuit operation [12] of radar threats in the MATLAB simulator. In order to implement the propagation of electromagnetic waves in the MATLAB simulator, we have used the models in References [4, 13, 14] for the loss and attenuation of a transmitted electromagnetic wave, and those in Reference [4] for Doppler and multi-path fading effects which a transmitted wave suffers.

There are generally two types of radar jamming, noise and deception. The noise jamming conceals the target signal with the intentionally radiated noise-like signal and the deception jamming deceives the tracking system of radar with the false information about the critical intelligence such as range, angle, or velocity of target. In the MATLAB simulator, we have implemented the functions of noise, range deceptive, velocity deceptive, angle deceptive, and noise-deception complex jamming [15,16], with consideration for jamming-to-signal power ratio (JSR) and burn-through range [15] under the self-protection scenario [17].

Fig. 3 shows the output screen of the MATLAB simulator when the complex jamming with barrage noise and angle deception jamming is applied. As the simulation progresses, the results of the output screen are updated according to the processing interval and speed. The upper-left and upper-right graphs display the radar scope and monopulse angle scope, respectively, those provide the range and angle tracking status. The bottom-left and bottom-right graphs show the received signal and its spectrum, respectively. The text boxes in the right side report the selected radar and jamming types, instantaneous tracking results, and root-mean-squared (rms) errors estimated in the whole simulation. The tracking results and rms estimation errors are stored separately in files, which can be used to investigate or analyze the effectiveness of jamming.



Radar Threat

Collected Information
Waveform type: cos
Pulse width: μs
Pulse power: dBm
PRI: μs
Carrier frequency: GHz
Scan period: s

Simulation Parameter
Processing time: s
Processing interval: s
Sampling rate: 4000 Samples / PRI
Processing speed: 1 ×

Type of Radar
● Search pulse radar
○ Search CW radar
○ Monopulse radar
○ Monopulse Doppler radar
○ Monopulse CW radar
Squint angle: deg
Filter bank size: 2 ^

CFAR
False alarm rate: 10 ^ (-)
Detection rate

H/W Parameter
Antenna
Beamwidth: deg
Maximum gain: dB
Gain control
● Limiter
○ AGC
Dynamic range: wide
Delay: 0.1 μs

IF. Mixer
Intermediate frequency: KHz
Amplifier gain: dB
Operating range: 0 dB, wide
Bandwidth (0 ~ 0) MHz, wide
Filter type: butterworth
Filter performance: good

Jammer

No Jamming ●
Burn through range: km
Jamming gain: dB
Duration: s
Delay jamming: s

Noise Jamming
Spot Noise ○
Number: 1
Barrage Noise ●
Band: - MHz

Range Deception
RGPO ○
RGPI ●
Jamming vel: m/s

Velocity Deception
VGPO ●
VGPI ○
Jamming acc: m/s²

Angle Deception
CE-PA ●
CE-NA ○
Jamming Vel: deg/s

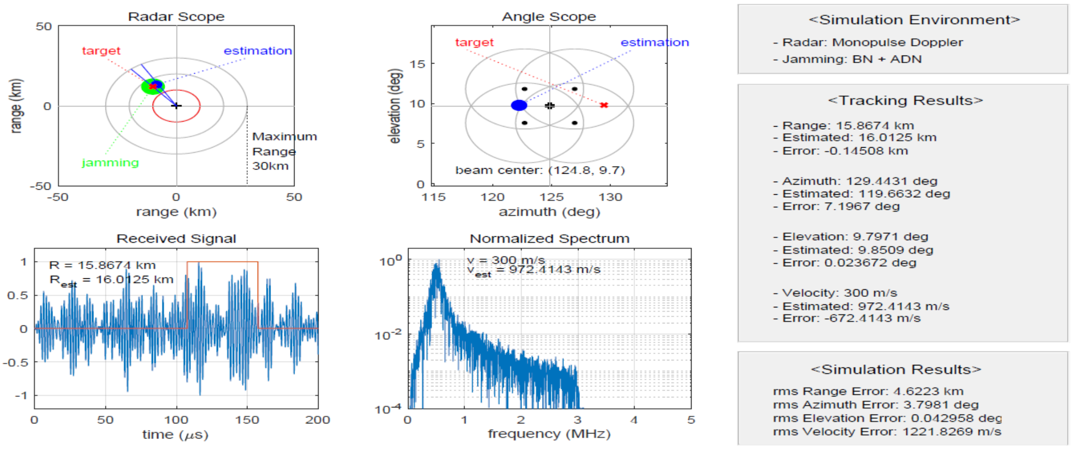
Aircraft

RCS: m²
Velocity: m/s
Initial location (, , 3) km
Direction: deg

Propagation

Temperature: ℃
ground type: soil
rainfall: mm/hr

Fig.2. Input screen of the MATLAB simulator



<Simulation Environment>
- Radar: Monopulse Doppler
- Jamming: BN + ADN

<Tracking Results>
- Range: 15.8674 km
- Estimated: 16.0125 km
- Error: -0.14508 km

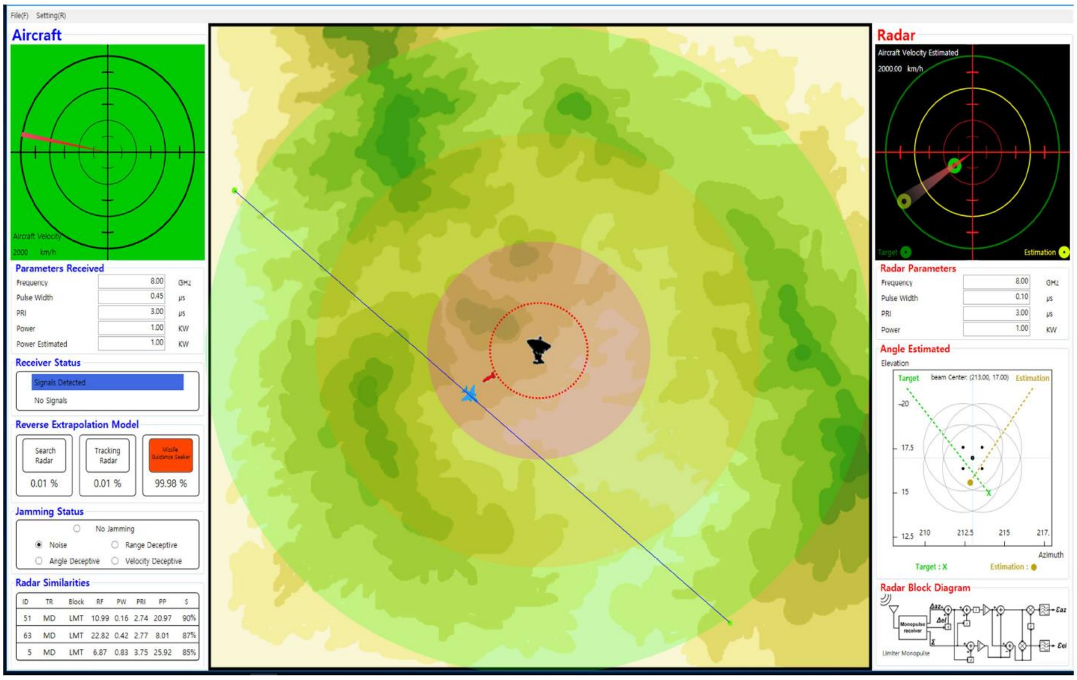
- Azimuth: 129.4431 deg
- Estimated: 119.6632 deg
- Error: 7.1967 deg

- Elevation: 9.7971 deg
- Estimated: 9.8509 deg
- Error: 0.023672 deg

- Velocity: 300 m/s
- Estimated: 972.4143 m/s
- Error: -672.4143 m/s

<Simulation Results>
rms Range Error: 4.6223 km
rms Azimuth Error: 3.7981 deg
rms Elevation Error: 0.042958 deg
rms Velocity Error: 1221.8269 m/s

Fig.3. Output screen of the MATLAB simulator



Parameters Received

Frequency	8.00	GHz
Pulse Width	0.45	μs
PRI	3.00	μs
Power	1.00	KW
Power Estimated	1.00	KW

Receiver Status

Signals Detected
No Signals

Reverse Extrapolation Model

Search Radar	Tracking Radar	Missile Guidance Seeker
0.01 %	0.01 %	99.98 %

Jamming Status

○ No Jamming
● Noise ○ Range Deceptive
○ Angle Deceptive ○ Velocity Deceptive

Radar Similarities

ID	TR	Block	RF	PW	PRI	PP	S
51	MD	LMT	10.99	0.16	2.74	20.97	90%
63	MD	LMT	22.82	0.42	2.77	8.01	87%
5	MD	LMT	6.87	0.83	3.75	25.92	85%

Radar Parameters

Frequency	8.00	GHz
Pulse Width	0.10	μs
PRI	3.00	μs
Power	1.00	KW

Angle Estimated

Fig.4. Screen capture of the simulator for the reverse extrapolation of radar threats and their verification

We utilize the MATLAB simulator to investigate how accurate the proposed reverse extrapolation model identifies the RF threat previously set, and also to ascertain how the radar threat responds to various electronic attacks. The characteristics of radar responses obtained by the simulator are efficiently used to improve the identification performance of the proposed reverse extrapolation.

B. Integrated Simulator for the Identification of Radar Threats and Their Verification

We have implemented the simulator for the reverse extrapolation of RF threats and their verification through jamming techniques, as depicted in Fig. 4. The simulator has been programmed using C# version 4.0, Visual Studio ® 2017 in .NET environment.

The simulator in Fig. 4 consists of the panels of RF threats, the electronic receiver of our aircraft agents, and the scenario display. The scenario panel in the middle of the screen displays a radar threat, our aircraft equipped with receiver, and their interactions according to radar's modes of searching, tracking, and missile seeker. The right panel of the simulator shows the information from a radar threat's perspective. The radar view in its top of the panel presents a target, i.e., aircraft, and a target deceived in case that a jamming is effective. Below the radar view, radio-active parameters emitting from the radar are listed. The parameters are frequencies, pulse width, pulse repetition interval, and pulse power. The angle estimation to the aircraft is shown in the screen of a unit MATLAB simulator plugged into the simulator. The bottom of the right panel illuminates a specific radar block diagram in use. The left panel of the simulator represents information received by our aircraft agents. The receiver view on its top presents the needle of an aero compass keeping track of a radar's location. The parameters acquired by the receiver are listed in the same order of radar view. The box below denotes whether or not radar signal is received.

Using our reverse extrapolation models of radar threats and the consolidation method for the unique identification of types of a radar, the accuracy of types of a specific radar is represented in percentage. Current jamming technique is specified in the form of option buttons. The left corner of the simulator shows a list of similar radars recommended from radar database.

The events of our simulator within a cycle happen in order. In preparation step, the capabilities and system block of a radar threat are selected, and our aircraft's path and it's jamming technique is preset. As starting simulation, our aircraft agent is proceeding in route previously defined, and the radar is beginning to search possible targets within its range. Our agents receive radioactive parameters through sensors, and then reversely extrapolate a radar threat given those parameters. To verify their extrapolation, they perform a jamming technique against the radar. And then, the radar simultaneously estimates our agent's position. Finally, our agents analyze jamming response and recommend similar radars considering the jamming response and a set of parameters received.

V. Experimental Results

Using the integrated EW simulator, we could perform two experiments and measure the performance of (1) the unique estimation of types of a radar threat, and (2) the recommendation of similar radars. In each experiment, we could set up various and realistic EW situations, and analyze the improvement of our agents' performance.

A. he Combined Prediction for the Types of Radar Threats

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., decision tree algorithm and naive Bayesian classifier, and implement k-means clustering algorithm using Euclidean distance and a neural network as unsupervised techniques [19].

We measure the performance of our agents with reverse models in terms of the correct identification of RF threats. The performance using each learning algorithm is depicted in Fig. 5. The average performance of four learning algorithms after 300 trials presents 87.00% for search radars, 88.52% for tracking radars, and 92.63% for missile seekers. In other words, each performance without integration shows ranging from 87% to 93%.

The average performance of combined predictions, as described in (1), using two, three, and four machine learning algorithms after 300 trials are shown in Fig. 6, Fig. 7, and Fig. 8, respectively.

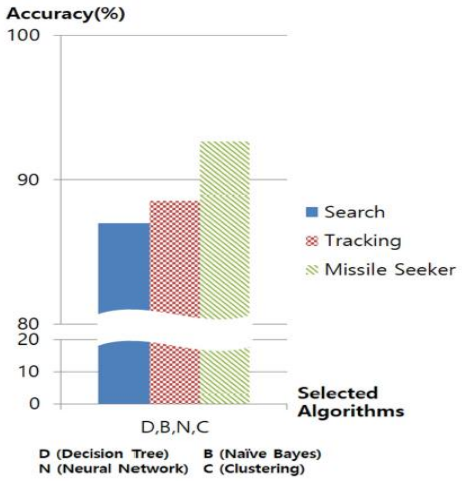


Fig.5. The performance on the types of an RF threat using a machine learning algorithm

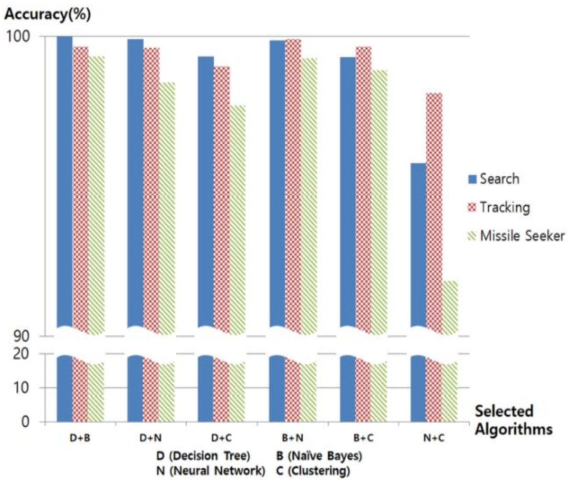


Fig.6. The combined prediction on the types of an RF threat using two machine learning algorithms

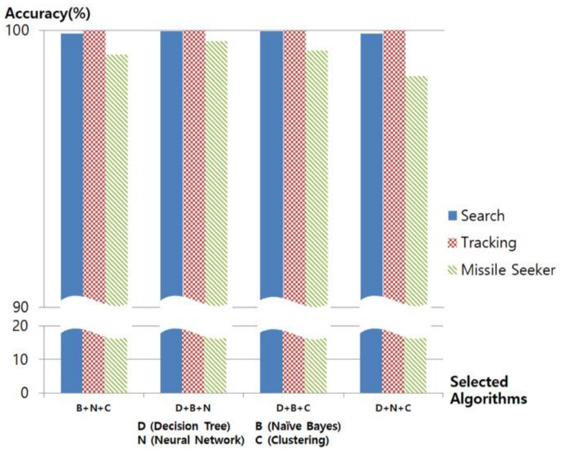


Fig.7. The combined prediction on the types of an RF threat using three machine learning algorithms

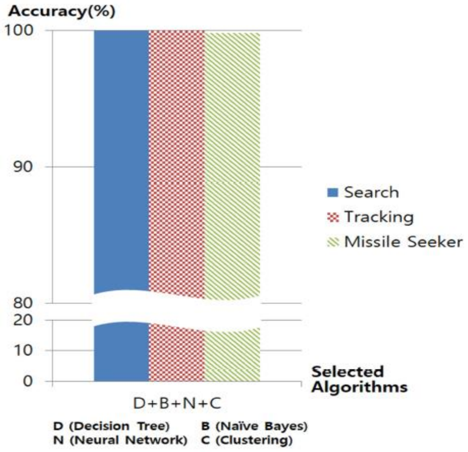


Fig.8. The combined prediction on the types of an RF threat using four machine learning algorithms

As machine learning algorithms are more combined for the reverse extrapolation of types of an RF threat, the accuracy of the threat identification is enhanced. The performance using four machine learning algorithms, as depicted in Fig. 8, presents the best performance such as 99.98% for search and tracking radars, and 99.84% for missile seekers. Given the results of performance, it turns out that the performance by a clustering algorithm was the worst while the performance using a decision tree algorithm was the best in a simulated EW domain. The integration of reverse models through Dempster-Shafer theory enables our aircraft agents to be almost perfectly aware of the types of radars under EW attack.

B. Recommendation of Radars from Radar DB

For the experiment, we assigned 200 instances into a radar database, where each instance could be a specification of practical radars. In an EW scenario, we measured similarities between an RF threat and all of radar instances, as described in (4), and obtained the average of best similarities given configurations of an RF threat over ten predefined scenarios. Since RF threats could be jammed by aircraft agents only during the RF threats kept tracking of our agents, the type of an RF threat was assumed to be a tracking radar or a missile seeker. The possible jamming techniques available to our aircraft agents were noise, range deceptive, angle deceptive, and velocity deceptive jamming. From an RF threat's perspective, the tracking type of the threat could be a discrete value of {Monopulse, Doppler} and the RF threat consisted of a nominal value of {AGC, Limiter} as blocks of hardware system. The average of best similarities in ten EW scenarios are summarized into Table 1.

For each row of Table 1, ten EW scenarios were tested and radar parameters received by our aircraft agents were randomly generated. Given threat configuration with numeric attributes of radar parameters and the threat response to the specific jamming, we could measure the similarities between the threat encountered and radar instances given database. As far as angle deceptive jamming, we implemented only Monopulse tracking radars, but no Doppler tracking radars. All of the similarities in Table 1 were distributed over 85%, regardless of configurations in our experiment. The computation of similarity enables our aircraft agents to be informed with realistic threat specification, even if EW scenarios construct a complex of combinations of RF threat components, parameters received, a specific jamming, and threat response to the jamming.

Table 1. The average of best similarities in ten EW scenarios

Jamming Types	Threat Types	Tracking Types	H/W Block	Similarity
Noise	Tracking	Monopulse	AGC Limiter	88.01 88.22
		Doppler	AGC Limiter	87.21 89.01
	M seeker	Monopulse	AGC Limiter	88.72 87.51
		Doppler	AGC Limiter	89.29 89.57
Range Deceptive	Tracking	Monopulse	AGC Limiter	88.07 87.08
		Doppler	AGC Limiter	88.89 88.57
	M seeker	Monopulse	AGC Limiter	88.69 86.85
		Doppler	AGC Limiter	88.02 85.90
Angle Deceptive	Tracking	Monopulse	AGC Limiter	90.94 90.32
	M seeker	Monopulse	AGC Limiter	90.60 88.49
Velocity Deceptive	Tracking	Monopulse	AGC Limiter	87.44 90.48
		Doppler	AGC Limiter	88.90 89.20
	M seeker	Monopulse	AGC Limiter	90.43 88.92
		Doppler	AGC Limiter	90.88 88.30

VI. CONCLUSION

Using a compilation technique, we generated multiple models of reverse extrapolation of RF threats. We measured the performance of our aircraft agents with reverse models in terms of the correct identification of RF threats. For the final decision on the types of the RF threat, we applied the Dempster's rule of combination to the accuracies of reverse extrapolation of the RF threat types. The performance we measured showed that the combined prediction to the threat types was more than 99%. As a consequence, the representative identification of RF threats, in case of several possible alternatives, makes our aircraft agents rapidly and effectively respond to the fatal condition, and fairly enhance their continual survival.

Our intelligent agents could calculate the similarities between the threat and a set of radar instances predefined in database, and, based upon the similarities, radar instances closest to the threat were recommended to our aircraft agents. In this experiment, we could verify that the specifications of radars recommended were very similar with those of the threats reversely extrapolated; more specifically, the values of similarity were larger than 85% in all of cases. As the radar database is filled with plenty of real-world specifications of radars in various scenarios, the survivability of our intelligent agents could be strengthened to realize their maximum potential, when they cope with a real EW situation.

We implemented a MATLAB simulator to investigate the tracking performances of radar threats and to verify the performance of the reverse extrapolation models in various EW situations. After confirming the estimation of hostile radars by using the MATLAB simulator, we eventually implemented the integrated EW simulator that displays interactions between our aircraft agents with receiver and the radar. The development of the EW simulator contributes to the advantages of specific scenario setup including realistic radar threats, performing various jamming techniques, and iterative testing and verifying our friendly agents' capabilities.

In our framework, we hope to deploy fully autonomous aircraft agents in EW simulated settings. We are going to expand our framework to decision-making of effective countermeasures to threats given situation at hand, based upon our efforts of autonomous situation awareness in this paper. In parallel, we will also develop a drone of agents, and design the testbed to repeatedly test their best formations for various types of jamming techniques.

Acknowledgment

This work has been supported by the Catholic University of Korea research fund (M2018B000200047) granted in the program year of 2018.

References

[1] A.E. Spezio, "Electronic warfare systems," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 633-644, 2002.

[2] 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.

[3] J. Thangarajah, L. Padgham, and S. Sardina, "Modelling situations in intelligent agents," in *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems (AAMAS '06)*, pp. 1049-1051, New York, NY, USA, 2006.

[4] S. Noh and S.R. Park, "Reverse modeling and autonomous extrapolation of RF Threats," *International Journal on Advances in Computer Science*, vol. 4, no. 18, pp. 89-97, Nov. 2015.

[5] G. Shafer, *A mathematical theory of evidence*, Princeton University Press, 1976.

[6] Q. Chen, A. Whitbrook, U. Aickelin and C. Roadknight, "Data classification using the Dempster–Shafer method," *Journal of Experimental and Theoretical Artificial Intelligence*, vol. 26, no. 4, pp. 493-517, 2014.

[7] 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.

[8] S. Kumar Das, "Modeling intelligent decision-making command and control agents: an application to air defense," *IEEE Intelligent Systems*, vol. 29, no. 5, pp. 22-29, 2014.

[9] Z. Han, "Modeling method and application of multi-agents in armored force operation simulation," in *Proceedings of Advanced Information Technology, Electronic and Automation Control conference*, pp. 2046-2049, Chongqing, China, Mar. 2017.

[10] B. Barshan and B. Eravci, "Automatic radar antenna scan type recognition in electronic warfare," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 4, pp. 2908-2931, Oct. 2012.

[11] M. McDonald and D. Cerutti-Maon, "Multi-phase centre coherent radar sea clutter modelling and simulation," *IET Radar, Sonar, and Navigation*, vol. 11, no. 9, pp. 1359-1366, Aug. 2017.

[12] S.R. Park, I. Nam, and S. Noh, "Modeling and simulation for the investigation of radar responses to electronic attacks in electronic warfare environments," *Security and Communication Networks*, ID 3580536, 13 pages, 2018.

[13] B.R. Mahafza, *Radar Systems Analysis and Design Using Matlab*, 3rd Ed., CRC Press, 2012.

[14] D.L. Adamy, *EW 101: A First Course in Electronic Warfare*, Artech House, 2015.

[15] R. Poisel, *Modern Communications Jamming Principles and Techniques*, Artech House, 2011.

[16] J.D. Townsend, M.A. Saville, S.M. Hongy, and R.K. Martin, "Simulator for velocity gate pull-off electronic countermeasure techniques," in *Proceedings of the IEEE Radar Conference*, pp. 1-6, Rome, Italy, May 2008.

[17] L. Surendra, S. Shameem, N. Susmitha, and T.S. Ram, "Analysis of self-screening jammer parameters with radar equation", *International Journal of Engineering Research and Applications*, vol. 4, no. 3, pp. 205-207, Mar. 2014.

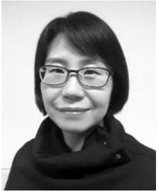
[18] I.H. Witten, E. Frank and M.A. Hall, *Data Mining: Practical machine learning tools and techniques*, 3rd edition, Morgan Kaufmann Publishers, 2011.

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

Authors' Profiles

Sanguk Noh received a B.S. in biology, an M.S. in computer science and engineering from Sogang University, Seoul, Korea, in 1987 and 1989, respectively, and a Ph.D. in computer science and engineering from the University of Texas, Arlington, TX, in 1999.

He is currently a professor in the School of Computer Science and Information Engineering at the Catholic University of Korea, Korea. He previously held research positions at the Agency for Defense Development, Korea (1989-1995), in the Center for Human-Computer Communication, Oregon Graduate Institute, Beaverton, OR (2000), and was an assistant professor in the Department of Computer Science at the University of Missouri, Rolla, MO (2000-2002). His research interests include intelligent real-time systems, machine learning, modeling and simulation, multi-agent systems, and knowledge management.



So Ryoung Park received the B.S. degree in electronics engineering from Yonsei University, Seoul, South Korea, in 1997, and the M.S.E. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 1999 and 2002, respectively.

Dr. Park was a Postdoctoral Research Fellow at the Statistical Signal Processing laboratory, Department of Electrical Engineering and Computer Science, KAIST, in 2002. In March 2003, she joined the School of Information, Communications, and Electronics Engineering, the Catholic University of Korea (CUK), Bucheon, South Korea, where she is currently a Professor. Her research interests include detection and estimation, communication theory, and statistical signal processing.

How to cite this paper: Sanguk Noh, So Ryoung Park, "Simulation for the Reverse Extrapolation of Radar Threats and their Verification", International Journal of Intelligent Systems and Applications(IJISA), Vol.11, No.7, pp.1-9, 2019. DOI: 10.5815/ijisa.2019.07.01