IEICE TRANS. INF. & SYST., VOL.E93–D, NO.3 MARCH 2010

PAPER

Optimal Decision-Making of Countermeasures by Estimating Their Expected Utilities*

So Ryoung PARK[†a)], ***Nonmember and*** **Sanguk NOH**[††b)], ***Member***

SUMMARY This paper investigates the autonomous decision-making process of the selection of alternative countermeasures against threats in electronic warfare settings. We introduce a threat model, which represents a specific threat pattern, and a methodology that decides the best countermeasure against real-time threats using the decision theory. To determine the optimal countermeasure, we model the probabilities of the effects of countermeasures, if executed, and combine the probabilities with their utilities. This methodology based upon the inductive threat model calculates the expected utilities of countermeasures which are applicable given a situation, and provide an intelligent command and control agent with the best countermeasure to threats. We present empirical results that demonstrate the agent's capabilities of choosing countermeasures to threats in simulated electronic warfare settings.

key words: *autonomous agent, decision theory, decision-making of countermeasures, electronic warfare settings*

1. Introduction

As countering threats in electronic warfare environments, a command and control agent needs to detect and classify them, and to autonomously execute countermeasures to them for the purpose of continually functioning despite potential danger. In our previous work [1], we have proposed a threat detection and classification mechanism through soft computing algorithms. To identify threats that our agents face, we endow them with a tapestry of reactive rules. The reactive rules are constructed by compiling threat systems and their attributes into state-action rules. The various compilations available constitute a spectrum of approaches to making identifications and classifications under various attacks in electronic warfare settings, and enable our agents to be aware of situations [2], [3].

To develop a comprehensive and rational command and control agent given an electronic warfare situation at hand, in this paper, we propose a methodology that autonomously decides the best countermeasures against real-time threats using decision theory [4]. The autonomous decision-making process of countermeasures involve tracking and identifying the state of a complex distributed environment, analyzing operational knowledge to predict what will happen in an imminent future state, and actively deciding an appropriate countermeasure to remove incoming threats. To determine the optimal countermeasure against threats, we model the effectiveness of countermeasures as their outcome probability, if executed, and then combine the probabilities with their utilities.

In order to decide countermeasures autonomously, it is necessary that the command and control agent estimates the effectiveness of each countermeasure on the present threat as accurately as possible. The effectiveness of a countermeasure means the actual capabilities of causing information damage in the detection or tracking sensor of a threat, and is estimated taking a lot of parameters into consideration. For example, let us assume that a radar homing missile is perceived and chaff and jammer are loaded in an aircraft [5]–[7]. The effectiveness of chaff is affected by the radar cross section (RCS) of the aircraft, the blooming time to create shielding cloud, the number of dipoles in cartridge, RCS of one dipole, resolution of tracking radar, weather conditions, speed of missile, and so on. In the case of jamming, the parameters are effective radiated powers (ERP) of radar and jammer, distance between radar and aircraft, the pulse width and bandwidth of radar signal, resolution of radar, etc. Since there are too many parameters to take into consideration at a time for deciding countermeasures and some parameters are actually unknown to the command and control agent of aircraft, the estimation of effectiveness is not a simple problem [5].

We provide our command and control agents with the ability to dynamically and rationally select countermeasures against threats. Our agents follow the decision theory [4], which calculates the expected utilities of alternatives. The agents will finally succeed in completing their tasks by executing the best countermeasure, which has the maximum expected utility. Since the properties of electronic warfare environments are unforeseen, partially accessible, and continuously changing, the protocol-based approaches [8] could not be applied to our setting. Applying the decision theory for the selection of countermeasures at military scenarios might be the first attempt to our best knowledge, and be a robust approach in battlefield situations.

In the following section, we will show clear factors that indicate the symptoms of various threat systems, de-

Manuscript received August 25, 2009.

[†]The author is with the School of Information, Communications, and Electronics Engineering, The Catholic University of Korea, Bucheon 420–743, Republic of Korea.

[††]The author is with the School of Computer Science and Information Engineering, The Catholic University of Korea, Bucheon 420–743, Republic of Korea (Corresponding author).

*This work has been supported by the Catholic University of Korea research fund granted in the program year of 2008, and by the Agency for Defense Development, Korea, under Grant UD070078ED "Autonomous Threat Detection and Classification," 2007.

a) E-mail: srpark@catholic.ac.kr

b) E-mail: sunoh@catholic.ac.kr

DOI: 10.1587/transinf.E93.D.560

scribe countermeasures to them, and then design the intelligent command and control agent, which is operational in electronic warfare settings. Section 3 presents our agent's decision-making process of the optimal selection of alternative countermeasures. Section 4 validates our framework empirically, and presents the experimental results. In conclusion, we summarize our results and discuss further research issues.

2. Designing Command and Control Agent in Electronic Warfare Settings

To improve the survivability of our agents in battlefield settings and successfully perform their mission, we extract features from various threat systems, define countermeasures to them, and design a command and control agent, which is autonomously operating [9], [10].

2.1 Analyzing Threats

Our agents detect their potential threats through their sensors: radar, laser, and infra-red. The threats could be outlined into 'terminal' and 'non-terminal' threats [6], [9], [10]. The terminal threats are intended to directly shutdown our agents, while the non-terminal threats are preliminary operations to enhance the capability of the terminal threat systems. The terminal threats consist of 'static' and 'mobile' lethal objects. The static terminal threats are antennas, power lines, buildings, and so on. On the other hand, the mobile terminal threats are missiles, guns, and rockets. The non-terminal threats include searching, tracking, and electronic countermeasures against communication systems [5], [11].

Some of the attributes contained in agents' knowledge bases (KBs) when they interact in battlefield scenarios are summarized in Table 1. The attributes in Table 1 are selected to effectively distinguish the threat types and the threat levels among all possible attributes. The attributes that should be considered regarding the threats detected by radar sensors are predominant and can be easily picked up, while those of the threats identified through laser sensors are usually limited. Since infra-red (IR) sensors have no range information and strongly depend on atmospheric conditions [6], the usage of IR sensors is restricted. However, the radar sensors are durable on all weather conditions and the attributes involving radar sensors are actively considered for the non-terminal and the terminal threats. As shown in Table 1, the attributes acquired from radar sensors are radar frequency, pulse width, pulse power, and pulse repetition frequency. The other attributes, i.e., pulse repetition frequency and guidance type, characterize the terminal threats confirmed by laser sensors.

2.2 Countermeasures

A countermeasure is a military system designed to prevent sensor-based weapons from acquiring or destroying a target. In this paper, chaff and radio frequency (RF) jamming is considered as RF countermeasures (or electronic countermeasure: ECM), and flare and IR jamming as IR countermeasures (IRCM).

Chaff is a passive RF countermeasure in which aircraft or other targets spread a cloud of small, thin pieces of aluminium, metalized glass fiber or plastic, which either appears as a cluster of secondary targets on radar screens or swamps the screen with multiple returns. Modern armed forces use chaff to distract radar-guided missiles from their targets. Most military aircraft have chaff dispensing systems for self protection.

RF jamming is a form of electronic warfare where jammers radiate interfering signals toward an enemy's radar, blocking the receiver with highly concentrated energy signals. The two main technique styles are noise techniques and repeater techniques. In this paper, it is assumed that RF

Table 1 Relevant attributes in electronic warfare settings.

Receiver Types	Attributes	Values	Threat Types
Radar	Radar Frequency	$30 - 8,000$ (MHz)	Non-Terminal
	Pulse Width	$0.8 - 5$ (ms)	
	Pulse Power	$10 - 500$ (KW)	
	Pulse Repitition Frequency (PRF)	$1 - 666$ (KHz)	
Radar	Radar Frequency	$8,000 - 40,000$ (MHz)	Terminal
	Pulse Width	$0.1 - 0.8$ (ms)	
	Pulse Power	$1 - 50$ (KW)	
	Pulse Repitition Frequency (PRF)	$333 - 1,000$ (KHz)	
Laser	Pulse Repetition Frequency (PRF)	$0.1 - 20$ (KHz)	Terminal
	Guidance Type	Range Finder/ Target Designator/ Beam Rider	
Infra-Red	Target Coordination	x, y, z	Non-Terminal/Terminal

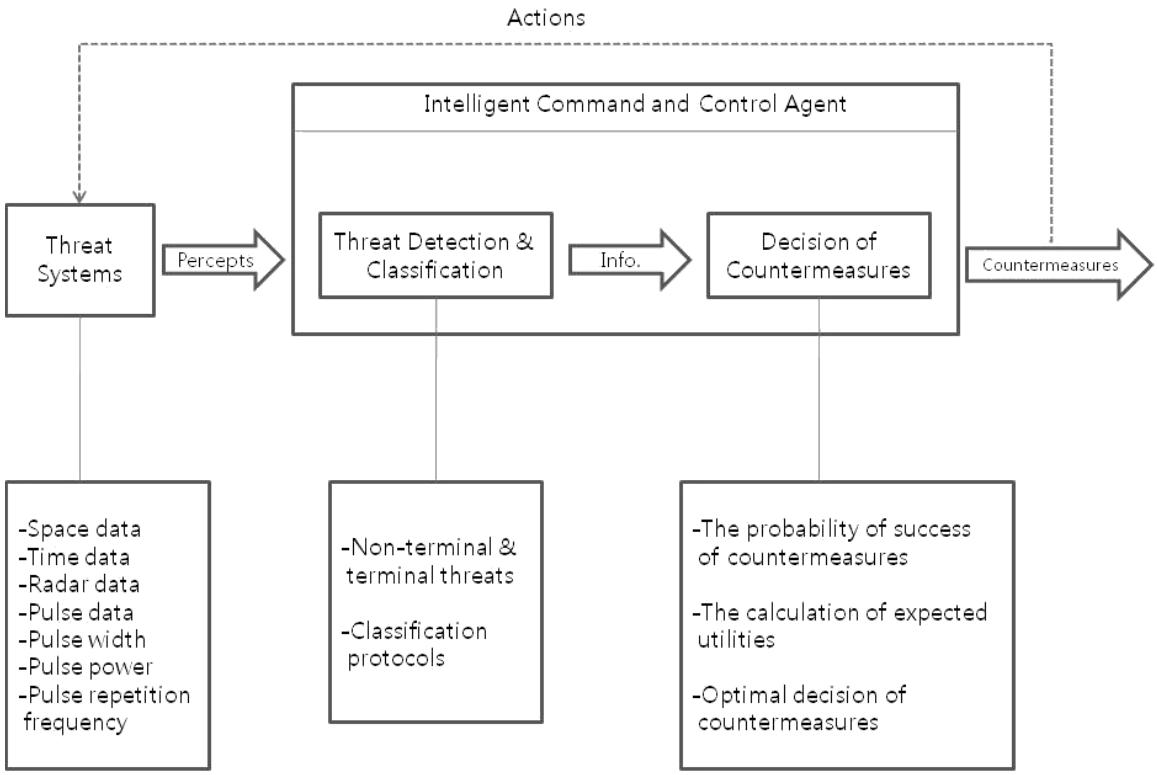

Fig. 1 The whole decision-making process of threat identification, classification, and the selection of countermeasures against threats.

jamming is performed in noise style on a single frequency.

Flare is an IRCM to counter an IR homing (heat seeking) missile. Flares are commonly composed of a pyrotechnic composition based on magnesium or another hot-burning metal with burning temperature equal to or hotter than engine exhaust, which makes the IR-guided missile to seek out the heat signature from the flare rather than the aircraft's engines.

IR jamming is an IRCM to provide incorrect steering cues or create plasma spark to missile seeker by emitting modulated energy. Generally, IR jamming systems are divided into three types:

- omnidirectional IRCM (wideband, low JSR)
- directed lamp IRCM (wideband, medium JSR)
- directed laser IRCM (high JSR)

where JSR is the jamming signal power to useful signal power ratio. Directed IRCMs (DIRCMs) are becoming operational, while mechanically modulated omnidirectional jammers still are effective against older IR homing missiles. It has been noticed that short laser pulses, focused on the detector, create a plasma spark within the seeker near the detector. The plasma may enhance jamming by pitting or scoring optics, creating debris, or upsetting electronics [6].

2.3 Designing Command and Control Agent

Our aim is to design autonomous agents which quickly response threat systems represented by the above attributes in Table 1, while operating in real-time electronic warfare settings. The first step towards this end is to integrate the symptoms of threat systems, and to detect and identify the threat systems themselves. We then classify the threats into terminal and non-terminal ones based upon categories compiled during off-line [1]. The final step of the command and control module is to dynamically decide the best countermeasure against threats using the computation of expected utilities in conjunction with on-line reasoning. The intelligent command and control agent to achieve our goal is illustrated in Fig. 1.

For the intelligent command and control agent, we propose a brokering agent architecture, as consisting of an information collecting and processing module that gathers the signatures of threat systems, an adaptive reasoning module that detects threat systems upon the pre-compiled protocols [†], and a decision theoretic module that finally executes the best countermeasure among alternatives. This architecture, as described in Fig. 1, allows our autonomous agents to quickly recognize a current situation using the pre-compiled protocols, and to actively remove potential adversities with robust autonomy through the calculation of expected utilities. The fast report of the current situation and the rational decision of the countermeasures provide the command and control agents with more prepared in an urgent situation and

[†]An information collecting and processing module and an adaptive reasoning module have been already developed in our previous work [1].

autonomous capability without relying on the operation of human beings.

3. Deciding Countermeasures Against Threats

To provide our agents with rationality, we use the decision theory [4] that combines preferences, i.e., utilities, with probabilities, in case of selecting countermeasures.

3.1 Calculating the Effectiveness of Countermeasures

In this section, we will propose a defining and calculating method of the effectiveness of countermeasures. We represent it as the probability of the incorrect detection of a threat guidance radar site, i.e., the signal power ratio of the countermeasure and the threat.

3.1.1 RF Countermeasure

At present, four groups of criteria have been determined that describe the special characteristics of electronic warfare as an element of information warfare related to the military use of electromagnetic emissions. These criteria include information, energy, tactical, and military/economic indicators that permit the evaluation of the effects of the level of RF countermeasures of electronic warfare. In this paper, considering the energy indicator for criteria on effectiveness of RF countermeasures, we express the effectiveness as the probability of an incorrect detection with regard to the power ratio of the countermeasure and the radar reflect signal.

In the radar operating modes considered, the Neyman-Pearson criterion is normally used, according to which, for a fixed probability of a false alarm P_{FA}, the probability of a missed target P_{miss} is minimized and the probability of a correct detection P_{D} is maximized. Considering the sample function of random noise as an additive white Gaussian noise, the likelihood ratio can be represented by

$$q = \sqrt{\frac{2E}{N_0}}, \tag{1}$$

where E is the signal energy and N_0 is the single-sided noise power spectral density. The likelihood ratio q is compared to the threshold h, which is determined by the value accepted as the probability of a false alarm P_{FA}.

In the case where the parameters of the signal are fully known and the noise is white, the probabilities of a correct detection and a false alarm are defined [12] by

$$P_{\mathrm{D}} = \frac{1}{2} - \Phi_0\left(\frac{h}{q} - q\right), \tag{2}$$

$$P_{\mathrm{FA}} = \frac{1}{2} - \Phi_0\left(\frac{h}{q}\right), \tag{3}$$

where

$$\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt.$$

For the conditions under consideration, the probability of a correct detection and a false alarm turn out to be linked by the relationship [5]

$$P_{\mathrm{D}} = P_{\mathrm{FA}}^{\frac{1}{1+0.5q^2}}. \tag{4}$$

The likelihood ratio q can be represented using JSR as

$$q = \sqrt{\frac{2n\tau_s \Delta f_s}{\mathrm{JSR}}}, \tag{5}$$

where $\mathrm{JSR} = P_j/P_s$ with the jamming signal power P_j and the reflected radar signal power P_s, τ_s is the pulse width, Δf_s is the bandwidth of radar signal, and n is the factor of radar performance. Using (4) and (5), we can have the expression of the probability of a correct detection

$$P_{\mathrm{D}} = P_{\mathrm{FA}}^{\frac{1}{1+n\tau_s \Delta f_s/\mathrm{JSR}}}, \tag{6}$$

and consequently, we have the effectiveness of RF countermeasures

$$E_{ff} = 1 - P_{\mathrm{FA}}^{\frac{1}{1+n\tau_s \Delta f_s/\mathrm{JSR}}}. \tag{7}$$

The well-known expression for JSR of RF jamming is

$$\mathrm{JSR}_R = \frac{ERP_j}{ERP_r} \frac{4\pi R^2}{\sigma_a} \frac{G_j}{G_r}, \tag{8}$$

where ERP_j is the ERP of jammer, ERP_r is the ERP of radar, R is the distance between radar and aircraft, σ_a is the RCS of aircraft, G_j is the antenna gain of jammer, and G_r is the antenna gain of radar. If the distance R between radar and aircraft is greater than the burn-through range R_{BT}, the effectiveness of RF jamming can be obtained by substituting JSR in (7) with (8). On the other hand, the effectiveness of RF jamming becomes zero if the aircraft enters into the burn-through range.

In the case of chaff, JSR can be interpreted as the RCS ratio of chaff cloud and aircraft [5]

$$\mathrm{JSR}_C = \frac{\sigma_c}{\sigma_a} l_r, \tag{9}$$

where σ_c is the average RCS of chaff, $l_r = c\tau_s/2$ is the resolution element of radar, and c is the light velocity. The average RCS of chaff cloud is calculated by

$$\sigma_c = n_j \sigma_j e_j, \tag{10}$$

where n_j is the number of chaff dipoles, σ_j is the RCS density of one chaff dipole, and e_j is the effective volume of chaff cloud varying with missile arrival time. The study about the accurate RCS density of one chaff dipole is essential for the effectiveness of chaff and has been investigated up to the present [13]. However, we will focus on the variation of the effective volume with time, since the response time may be more important in the decision-making of a countermeasure. The effective volume can be assumed to be rapidly increased, maximized at a time point, maintained for some duration, and decreased to zero, so that we model the

Table 2 The influence of IR countermeasures on IR seekers.

Seeker Type	S_1	S_2	S_3	S_4
Flare	strong	medium	week	no
Omnidirectional	strong	strong	medium	week
Directed Lamp	strong	strong	strong	medium
Directed Laser	strong	strong	strong	strong

effective volume mathematically using the beta functions as

$$e_j = \begin{cases} f_{\beta_r}(t/t_{\max}), & t < T_0, \\ 1, & T_0 \le t < T_0 + D, \\ f_{\beta_f}(t/t_{\max}), & T_0 + D \le t < t_{\max}, \\ 0, & t \ge t_{\max}, \end{cases} \tag{11}$$

where $f_\beta(x) = B_{2,\beta}(x)/B_{2,\beta}(\beta^{-1})$, T_0 is the maximum point, D is a maintenance duration, $t_{\max}$ is a simulation bound which can be related with the number of ejected packet, $\beta_r = t_{\max}/T_0$ is an increasing rate, β_f is a decreasing rate, and

$$B_{\alpha,\beta}(x) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \tag{12}$$

$0 < x < 1, \alpha > 0, \beta > 0$ is the beta distribution function [14]. In particular, D and β_f are changed with the degree of wind velocity and rainfall.

3.1.2 IR Countermeasure

The effectiveness of IR countermeasures is greatly influenced by the IR seeker type of missile. Since the amount of information damage at IR seeker by a countermeasure can be hardly modelled in numerical formula, we consider the statistical model for the effectiveness reflecting the mutual influence between four types of IR countermeasure in aircraft and four types of IR seeker in missile. The influence of IR countermeasures on IR seekers is shown in Table 2, where S_i, $i \in \{1, 2, 3, 4\}$ indicates an IR seeker type and the larger i means the better performance of S_i.

Flares are effectual as an IR countermeasure if an IR homing missile arrives at one of ejected flares, that is, $E_{ff} = 0$ if $T_F V_M < D_{AM}$. Here, T_F is the duration of a flare, V_M is the velocity of missile, and D_{AM} is the distance between aircraft and missile. In the case of three types of IR jamming, $E_{ff} = 0$ if $R_I < D_{AM}$, where R_I is the maximum range of an IR jammer.

3.2 Deciding Countermeasures

To be rational in decision-theoretic sense, the agents follow the principle of maximum expected utility (PMEU) [4]. We will show how PMEU can be implemented in the decision-making process of the selection of countermeasures under uncertainty. Our agents equipped with PMEU will select the most appropriate countermeasure to effectively remove threats.

We will use the following notation:

- a set of agents: $N = \{n_1, n_2, \ldots\}$;
- a set of actions of agent n_i, $n_i \in N$: $A_{n_i} = \{a_i^1, a_i^2, \ldots\}$;
- a set of possible world states: $S = \{s_1, s_2, \ldots\}$.

The expected utility of the best action, α, of agent n_i, arrived at using the body of information E, and executed at time t, is given by [†]

$$EU(\alpha|E,t) = \max_{a_i^j \in A_{n_i}} \sum_k P(s_k|E,t,a_i^j) U(s_k) \tag{13}$$

where

- $P(s_k|E,t,a_i^j)$ is the probability that a state s_k will obtain after action a_i^j is executed at time t, given the body of information E.
- $U(s_k)$ is the utility of the state s_k.

For the purpose of formalizing the decision-making problem of selecting countermeasures against threats, we should model probabilities and utilities in (13). In our model, for example, the probability that a countermeasure would be effective is assumed to depend on jamming signal power, useful signal power reflected, distance between the radar and aircraft, and so on, when jamming countermeasures are executed, as summarized in (7) and (8). The utility that denotes the desirability of a resulting state after a countermeasure is executed can be assigned by a single number considering the type of receivers. We will give the concrete example of the computation of expected utilities with four countermeasures in the following section.

4. Simulation Tests and Experimental Results

The experiments in this section are designed (i) to generate the effectiveness of countermeasures to threats, and (ii) to evaluate the performance of the decision-making of countermeasures against them. First, we generate and validate the probabilities of effectiveness, when several countermeasures are applied to a specific threat. In the second experiment, as combining the probabilities with utility theory, we measure a decision-theoretic agent's performance in terms of the expected utilities of the best countermeasures selected given a situation. The agent's performance in the experiments were gathered on an Intel® Core™2 Duo 2.66-GHz processor machine.

4.1 Effectiveness of Countermeasures

The effectiveness of RF jamming is determined by (7), (8), and burn-through range. Figure 2 is an example of the JSR and effectiveness curves of RF jamming when $\sigma_a = 10\text{m}^2$, $ERP_jG_j = 25\,\text{dB}$, $ERP_rG_r = 110\,\text{dB}$, $P_{\text{FA}} = 10^{-3}$, and $n = 30$. Assuming that $R_{\text{BT}} = R|_{\text{JSR}=0\text{dB}}$, the corresponding burn-through range is $R_{\text{BT}} = 15.863\,\text{km}$ in this example. Figure 3 is the effectiveness of RF jamming when the factor n of radar performance varies and other parameters are the same as in Fig. 2. For larger n, the performance of radar

[†]Our notation follows [4].

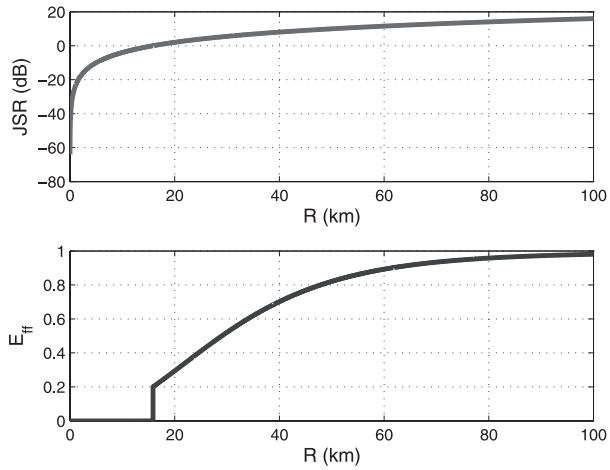

Fig. 2 The JSR and effectiveness of RF jamming.

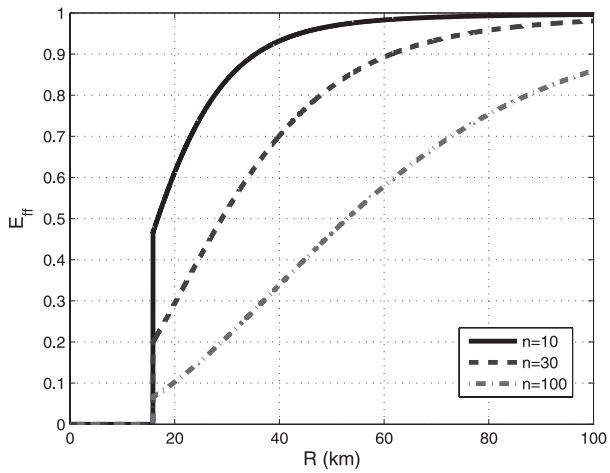

Fig. 3 The effectiveness of RF jamming with various radar performance.

detection and tracking is higher, and consequently, the effectiveness of RF jamming is lower at the same distance from radar.

The effectiveness of chaff generated using (7) and (9)–(11) is shown in Fig. 4 when $t_{\max} = 50\,\text{s}$, $T_0 = 0.1t_{\max}$, $P_{\text{FA}} = 10^{-6}$, $\sigma_j = 0.01\text{m}^2$, and $n_j = 100$. D and β_f are classified with six levels and determined by the weather conditions as shown in Table 3. For example, the effectiveness of chaff at 20 s after ejecting is about 1 in slight rain or breeze, but it is 0.9 in slight rain and breeze, 0.2 in rain or wind, and 0 in heavy rain or gale.

When the several effectual countermeasures are applied to one threat in electronic warfare settings, the effectiveness of the combined countermeasures can be calculated by

$$E_{ff,\text{Total}} = 1 - \prod_{i=1}^{N}(1 - E_{ff,i}), \tag{14}$$

where N is the number of effectual countermeasures and $E_{ff,i}$ is an effectiveness of the ith countermeasure. Figure 5 is the effectiveness of combined countermeasures when chaff and RF jamming are concurrently applied to a

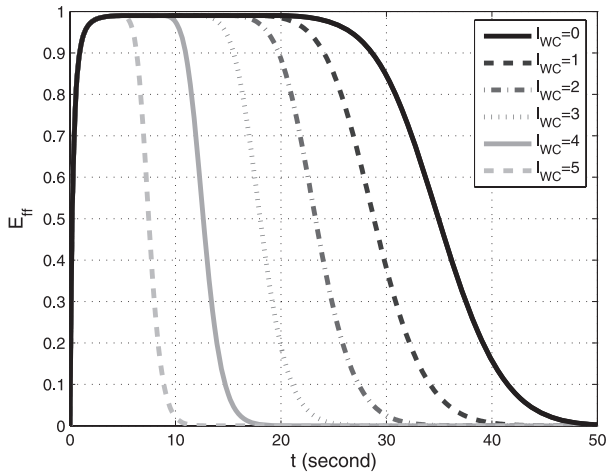

Fig. 4 The effectiveness of chaff with various weather conditions.

Table 3 Maintenance duration and decreasing rate of chaff cloud determined by the level of weather condition l_{WC}.

l_{WC}	Weather	D	β_f
0	No wind and no rain	$3.0t_{\max}$	10
1	Slight rain or breeze	$2.6t_{\max}$	15
2	Slight rain and breeze	$2.1t_{\max}$	22
3	rain or wind	$1.5t_{\max}$	32
4	rain and wind	$0.8t_{\max}$	50
5	Gale or heavy rain	0	75

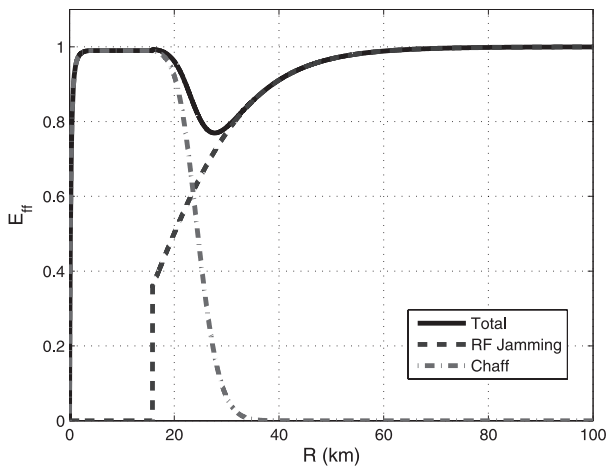

Fig. 5 The effectiveness of a combined RF countermeasure.

radar homing missile. For RF jamming, we set the parameters as $\sigma_a = 10\text{m}^2$, $ERP_jG_j = 25\,\text{dB}$, $ERP_rG_r = 110\,\text{dB}$, $P_{\text{FA}} = 10^{-6}$, and $n = 30$. For chaff, $t_{\max} = 50\,\text{s}$, $T_0 = 0.1t_{\max}$, $\sigma_j = 0.01\text{m}^2$, $n_j = 100$, $l_{\text{WC}} = 1$, and $V_M = 850\,\text{m/s}$. In this figure, we can see that chaff cloud is more effective than RF jamming at about 0~20 km, however, at further distance than about 25 km, RF jamming is a better countermeasure than chaff. The total effectiveness of chaff and RF jamming is obtained by (14) and represented as the solid line in Fig. 5.

Figure 6 shows the effectiveness of IR countermeasures with various seeker type of missile when $V_M = 850\,\text{m/s}$,

Table 5 The payoff matrix of utilities in electronic warfare settings.

Scenario Types	The type of receivers			The utilities of countermeasures			
	RWR	MWR	LWR	Chaff	RF Jamming	Flare	IR Jamming
1	√			0.393	0.551	-	-
2		√		-	-	0.393	0.551
3			√	-	-	-	-
4	√	√		0.393	0.551	-	-
5	√		√	0.393	0.551	-	-

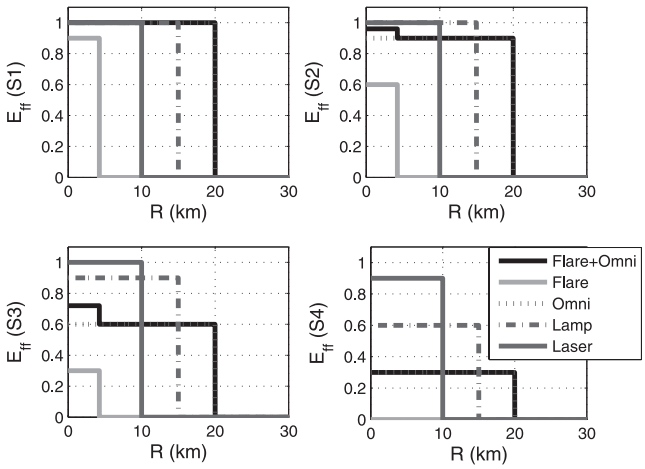

Fig. 6 The effectiveness of various IR countermeasures.

Table 4 An example of the influence of IR countermeasures on IR seekers.

Seeker Type	S_1	S_2	S_3	S_4
Flare	0.9	0.6	0.3	0.0
Omnidirectional	1.0	0.9	0.6	0.3
Directed Lamp	1.0	1.0	0.9	0.6
Directed Laser	1.0	1.0	1.0	0.9

the duration of flare is 5 s, the range of IR jamming is 10, 15, and 20 km for omnidirectional, directed lamp, and directed laser jamming, respectively. We also assume that the direction of arrival is perfectly estimated and the specific influences of countermeasures on IR seekers are such values as in Table 4. For example, the effectiveness of flare is 0.3, that of omnidirectional jamming is 0.6, and that of the combined countermeasures of flare and omnidirectional jamming is 0.72 if the seeker type is S_3 and the distance between aircraft and IR homing missile is less than 4.25 km.

4.2 Example Scenario

As a simple example let us consider an electronic warfare scenario. This scenario has a command and control agent confronting a specific threat. The mission of our agents is to autonomously decide and execute their countermeasures to a specific threat. The agent is assumed to be equipped with four countermeasures, $A_{n_i} = \{chaff, RF\ jamming, flare, IR\ jamming\}$. In this example scenario, our agent identifies a threat through only a radar warning receiver (RWR), which is the scenario 1 in Table 5. According to the types of receivers, the countermeasures that can be applicable are limited, and, in this case, only $chaff$ and $RF\ jamming$ can be useful, as described in Table 5.

Given a situation at hand, our agents following decision theory should choose a countermeasure that maximizes their expected utility, as described in (13). In this example scenario, the situation is characterized by the attributes, i.e., PW=50 μs, PA=400 kW, wind velocity=26 ms, and rainfall=15 mm. First, the probabilities that each countermeasure would be successful can be acquired through the computation in (7)–(9) as follows:

- $P(Result_s(chaff)|Do(chaff), E, t) = 0.990$;
- $P(Result_s(RF\ jamming)|Do(RF\ jamming), E, t) = 0.968$.

where $Result_s(chaff)$ is a possible outcome state that $chaff$ could be effective, and $Do(chaff)$ is the proposition that $chaff$ countermeasure is executed in the current state given the evidence E.

Second, the utility that denotes the desirability of a resulting state after a countermeasure is executed can be summarized in Table 5. The utilities of $RF\ jamming$ and $IR\ jamming$ are greater than those of $chaff$ and $flare$, and their specific utility values can be obtained from the utility function, $1/(1 - e^{-\lambda x})$, where λ is the constant of 0.1 and x is a real value between 1 and 10, which is corresponding to one of countermeasures. When no countermeasures are successful, the utility value that our agents can have is assumed to be 0.095, where the value of x is 1.

Thus, the expected utilities of the command and control agent's alternative countermeasures, as defined in (13), are:

- $EU(chaff|E, t) = 0.990 \times 0.393 + 0.010 \times 0.095 = 0.390$;
- $EU(RF\ jamming)|E, t) = 0.968 \times 0.551 + 0.032 \times 0.095 = 0.564$.

In this example scenario, therefore, our command and control agents will take the action of $RF\ jamming$ as their best countermeasure.

4.3 Performance of the Decision of Countermeasures

To evaluate the quality of the decision-making process of countermeasures against threats in electronic warfare settings, the resulting performance was expressed in terms of the cumulative expected utilities. The cumulative expected utilities are defined as the sum of expected utilities after 30

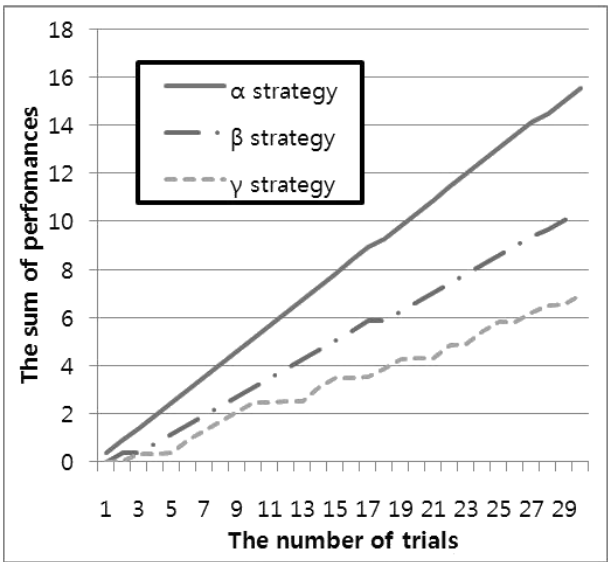

Fig. 7 The sum of performances (expected utilities) vs. the number of trials for the selection of alternative countermeasures.

selections of countermeasures have been made. The average of the cumulative expected utilities through ten sets of 30 selections was summarized in Fig. 7.

In this experiment, the strategies for the selection of countermeasures are as follows:

- α strategy: the selection of the countermeasure that has the highest expected utility;
- β strategy: the selection of the countermeasure that has the highest probability representing its successfulness, when it is executed;
- γ strategy: the random selection of the countermeasure.

As we expected, in Fig. 7, the performance achieved by our agents following decision theory was better than those of the agents guided by the random selection strategy and by the β strategy. The performance of β strategy was better than that of the random selection strategy, but was worse than that of α strategy. Compared with the performance, 10.438, of the agents with β strategy, the performance, 15.543, of our agents was increased by 48.89%.

5. Conclusion

In time-critical settings, autonomous agents need to quickly recognize a given situation, and to rationally react to it. Our work contributes to situation awareness, when robust autonomy is crucial. In this paper, we present a fully autonomous command and control agent in electronic warfare settings. From the command and control agent's perspective, we showed the autonomous decision-making process of the selection of alternative countermeasures against threats.

First, we analyzed threat systems into a set of attributes to formulize their model. In order to estimate how much effective a countermeasure would be, then, we defined the effectiveness of countermeasures and proposed the calculation method of the effectiveness. Further, our agents were capable of choosing and executing countermeasures to threats, as maximizing their expected utilities, to be rational in dynamic electronic warfare settings.

We tested our agent's performance in simulated electronic warfare settings. Considering the specifications of the threat, aircraft, and weather condition, the effectiveness of each countermeasure was calculated at a fixed distance between the threat and aircraft. The preliminary experiments revealed that the effectiveness of countermeasures were useful to accurately predict the resulting effectiveness of the countermeasures, and the computation of expected utilities made our agents rationally operational in dynamic environments.

As part of ongoing work, we are performing a set of experiments with all possible configurations of threat systems, and are implementing threat simulator. We will integrate various threat systems into a unified battlefield scenario and continuously test our agent's rationality with a tapestry of scenarios. We expect to improve the capability of command and control agents through our future work and to apply our framework to other time-critical domains.

References

[1] S. Noh, "Autonomous situation awareness through threat data integration," Proc. 2007 IEEE International Conference on Information Reuse and Integration, pp.550–555, Aug. 2007.
[2] D.J. Bryant, F.M.J. Lichacz, J.G. Hollands, and J.V. Baranski, "Modeling situation awareness in an organisational context: Military command and control," A cognitive approach to situation awareness: Theory and application, S. Banbury and S. Tremblay, eds., Chapter 6, Burlington, VT: Ashgate Publishing Company, 2004.
[3] J. Patrick and N. James, "A task-oriented perspective of siutation awareness," in A cognitive approach to situation awareness: Theory and application, ed., S. Banbury and S. Tremblay, Chapter 4, Ashgate Publishing Company, Burlington, VT, 2004.
[4] S.J. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 2nd Edition, Chapters 13–17. Prentice-Hall, Upper Saddle River, New Jersey, 2003.
[5] S.A. Vakin, L.N. Shustov, and R.H. Dunwell, Fundamentals of Electronic Warfare, Artech House, London, 2001.
[6] J. Heikell, Electronic Warfare Self-Protection of Battlefield Helicopters: A Holistic View, Helsinki University of Technology, doctoral dissertation, 2005.
[7] L.D. Kennedy, C.R. Patterson, and D.C. Munshower, "F/A-18 electronic warfare suite cost and operational effectiveness analysis methodology: Phase 1 - radio-frequency countermeasures," Johns Hopkins APL Technical Digest, vol.18, no.1, pp.59–68, 1997. Available: http://techdigest.jhuapl.edu/td1801/kennedy.pdf
[8] A.S. Rao and M.P. Georgeff, "BDI agents: From theory to practice," Proc. 1st International Conference of Multiagent Systems, pp.312–319, July 1995.
[9] Advanced EW protection for maximum survivability, Northrop Grumman, AN/APR-39B(V)2, Suite of integrated sensors and countermeasures (SISCM).
[10] Aircraft survivability equipment (ASE): Ensuring lethality and dominance of Army aviation over tomorrow's battlefield, Association of the United States Army, July 2002.
[11] H. Zhongwen and W. Zongxiao, Sources and Techniques of Obtaining National Defense Science and Technology Intelligence, Kexue Jishu Wenxuan Publishing, Beijing, 1991. Available: http://www.fas.org/irp/world/china/docs/

[12] L.L. Scharf, Statistical Signal Processing: Detection, Estimation, and Time Series Analysis, Addison-Wesley, 1991.
[13] P. Pouliguen, O. Bechu, and J.L. Pinchot, "Simulation of chaff cloud radar cross section," Proc. IEEE Antennas and Propagation Soc. Int. Symp., vol.3A, pp.80–83, July 2005.
[14] A. Papoulis and S.U. Pillai, Prabability, Random Variables, and Stochastic Processes, 4th Edition, McGraw-Hill, New York, 2002.

So Ryoung Park received the B.S. degree in electronics engineering from Yonsei University, Seoul, Korea, in 1997, and the M.S.E. and Ph.D. degrees in electrical engineering from KAIST, Daejeon, Korea, in 1999 and 2002, respectively. Dr. Park is currently an associate professor in the School of Information, Communications, and Electronics Engineering at the Catholic University of Korea (CUK), Bucheon, Korea. She was a Research Scientist at the Statistical Signal Processing laboratory, Department of Electrical Engineering and Computer Science, KAIST, in 2002. Her current research interests are in mobile communications and statistical signal processing with emphasis on spread spectrum communications. She was the recipient of a Silver Prize and a Gold Prize at Samsung Humantech Paper Contest in 1999 and 2001, respectively.

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 an associate 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 decision theory, multi-agent systems, knowledge management, machine learning, and intelligent real-time systems.