Roponen, Juho; Ríos Insua, David; Salo, Ahti

**Adversarial risk analysis under partial information**

*Published in:*
European Journal of Operational Research

*DOI:*
10.1016/j.ejor.2020.04.037

Published: 16/11/2020

*Document Version*
Publisher's PDF, also known as Version of record

*Published under the following license:*
CC BY-NC-ND

*Please cite the original version:*
Innovative Applications of O.R.

Adversarial risk analysis under partial information

Juho Roponen a,∗, David Ríos Insúa b, Ahti Salo a

a Systems Analysis Laboratory, Department of Mathematics and Systems Analysis Aalto University School of Science, PO Box 11100 Aalto FI 00076, Finland
b KICAT–Institute of Mathematical Sciences, Nicolás Cabrera, n 13-15 28049 Madrid, Spain

A R T I C L E   I N F O

Article history:
Received 18 February 2019
Accepted 20 April 2020
Available online 28 April 2020

Keywords:
Risk analysis
Decision analysis
Game theory
Stochastic dominance
Combat modeling

A B S T R A C T

Adversarial risk analysis provides one-sided decision support to decision makers faced with risks due to the actions of other parties who act in their own interest. It is therefore relevant for the management of security risks, because the likely actions of the adversary can, to some extent, be forecast by formulating and solving decision models which explicitly capture the adversary’s objectives, actions, and beliefs. Yet, while the development of these decision models sets adversarial risk analysis apart from other approaches, the exact specification of the adversary’s decision model can pose challenges. In response to this recognition, and with the aim of facilitating the use of adversarial risk analysis when the parameters of the decision model are not completely known, we develop methods for characterizing the adversary’s likely actions based on concepts of partial information, stochastic dominance and decision rules. Furthermore, we consider situations in which information about the beliefs and preferences of all parties may be incomplete. We illustrate our contributions with a realistic case study of military planning in which the Defender seeks to protect a supply company from the Attacker who uses unmanned aerial vehicles for surveillance and the acquisition of artillery targets.

© 2020 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license. (http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. Introduction

As a growing field of research, Adversarial risk analysis (ARA) (Banks, Aliaga, & Ríos Insúa, 2015) provides one-sided decision support to a decision maker who is faced with risks that depend on the decisions of other self-interested parties. This makes ARA relevant for the analysis and management of security risks, including those of terrorism, military operations and cyber threats. There are numerous reported ARA applications in areas such as anti-piracy (Sevillano, Ríos Insúa, & Ríos, 2012), counter terrorism (Ríos & Insúa, 2012), combat modeling (Roponen & Salo, 2015), and anti-IED war (Wang & Banks, 2011), for instance.

Specifically, ARA helps characterize the likely actions of all parties by building and analyzing multi-agent representations of the decision problem, taking into account their values, objectives, goals, capabilities and beliefs of the parties involved. Particular attention is paid to modeling the information on the basis of which the parties, referred to as adversaries, make their decisions. The aim is to build realistic models which, unlike most game theoretical analyses (Antos & Pfeffer, 2010; Ozdaglar & Monache, 2011), do not necessitate far-reaching and partly unrealistic assumptions about common knowledge which shared by all parties.

While the modeling of the adversaries’ decision processes makes ARA a powerful approach, there are notable challenges, too. In particular, it can be difficult to produce accurate estimates about how the adversary’s preferences and beliefs evolve over time. This could be the case, for instance, in situations where two adversaries, the Defender (‘she’) and the Attacker (‘he’), of which the Defender first chooses what countermeasures she will adopt in her defence, thereafter the Attacker, knowing the Defender’s choice, updates his beliefs and proceeds by deciding how to attack (Xu & Zhuang, 2016). These difficulties notwithstanding, attempts to building realistic representations of the intertwined decision problem should be made, because such representations can yield valuable insights and because the reliance on overly simplistic models of the adversary’s preferences will lead to sub-optimal countermeasures (Nikoofal & Zhuang, 2015).
In this paper, we develop conceptual, mathematical and computational methods based on the concepts of partial information and stochastic dominance to identify which of the adversaries’ decisions are non-dominated and therefore plausible (Levy, 1992). The practical relevance of these methods stems from the fact that the set of these non-dominated decisions tends to be much smaller than the set of all possible decisions. Thus, they provide useful decision support even in situations where complete information about the adversaries’ utilities and/or beliefs cannot be obtained. Specifically, we allow for the possibility that there is only partial information about the preferences and beliefs of the Attacker (or even about the the Defender), operationalized through subsets of probability distributions and multi-attribute utility functions. As it turns out, this approach is quite flexible and suitable for providing informative decision support. We note that what we call partial information differs from what is understood by Rothschild, McBay, and Guikema (2012) who examine situations where the Attacker can only partially observe the Defender’s defence decision.

We illustrate our methods in the light of a sequential defend-attack game, as such games are particularly important in the security domain (Brown, Carlyle, Salmerón, & Wood, 2006; Zhuang & Bier, 2007). Previously, stochastic dominance has been applied to examine both simultaneous or continuous games, see Fishburn (1978) and Rass, König, and Schauer (2017). However, as noted by Fishburn (1978), simultaneous games do not always have realistic properties and consequently simple game theoretic solutions may not provide meaningful decision support. For example, in the continuous game considered by Rass et al. (2017), the Attacker’s decision problem is modeled so that the Attacker only seeks to cause maximal harm to the Defender, which effectively reduces the problem to a two-player zero sum game.

For completeness, we first review the Bayesian Nash equilibrium solution which is used in (i) methods which rely on common prior probability distributions over players’ types and (ii) the standard ARA solution which uses probability distributions to model uncertainties about the adversary’s preferences and beliefs. Then, we present our key methodological contributions in two variants, starting from the situation in which there is incomplete information only about the preferences and beliefs of the adversary (in our case the Attacker), modeled though sets of utility functions and probabilities. We then consider the situation in which the information about the Defender’s (own) preferences and beliefs, too, may be incomplete, using stochastic dominance to produce meaningful analyses (Shaked & Shanthikumar, 2007). Finally, we show how the partial information approach can be extended to analyze sequential games in so-called regular influence diagrams.

We also present a realistic case study to illustrate how our methods can be applied to different kinds of sequential problems. In our case study, the Defender seeks to determine an efficient portfolio of countermeasures to protect a supply company against the Attacker’s unmanned aerial vehicle (UAV) reconnaissance and the subsequent specification of artillery targets. The Attacker, in turn, seeks to choose UAV and artillery systems which are cost-efficient in responding to the Defender’s countermeasures. We also discuss other security and military problems which are amenable to our methods.

2. Bayesian models

Adversarial problems are often modeled as two-player games (Cox, Jr, & Anthony, 2009; Washburn, Kress et al., 2009). Real world multi-agent decision problems can often be modeled as games of incomplete information, meaning that there are some players who do not know all the rules of the game, such as the capabilities, utilities and decision processes of the other players. In stochastic games there are uncertain chance events, such as weather or the outcome of a military combat. Furthermore, in games of imperfect information, there are players who cannot observe the previous actions of the other players and/or the outcomes of random events before it is their turn to act.

By far the most common approach to solving games of incomplete information is based on the Bayesian Nash equilibrium. Modeling the game as what is commonly known as a Bayesian game transforms the game of incomplete information into a stochastic game of imperfect information. In a Bayesian game, the type of each player is defined by his/her utilities, beliefs, decision alternatives, available resources, etc. Every player can observe his/her own type but not the types of other players. (Harsanyi, 1967)

In order to solve the stochastic game, it is necessary the make assumptions about the players’ types as well as their beliefs concerning each others’ types, formalized through prior probability distributions. In the traditional game theoretical approach, the players are assumed to have common knowledge about these prior distributions (Bier, Olveros, & Samuelson, 2007). It is even possible to derive the prior distributions based on a level-k approach (Rothschild et al., 2012). While choosing the right probability distributions is important and has both practical and philosophical implications, the question of where these distributions come from does not affect how the game is solved.

In ARA applications, in contrast, the prior distributions are based on the subjective estimates of the player whose decisions are being supported and who seeks to choose the best decision alternative(s) under adversarial uncertainty (Rios Insua, Rios, & Banks, 2009).

2.1. Influence diagrams

We visualize ARA problems using bi-agent (or even multi-agent) influence diagrams (Banks et al., 2015). In an influence diagram, rectangular nodes indicate decisions, circular nodes depict uncertain chance events, and hexagonal nodes correspond to utilities. Directed arcs are employed to connect the nodes so that continuous arcs represent probabilistic dependencies and dashed arcs represent the information that is available at decision nodes. Based on information about (i) the adversaries, (ii) the order in which they make decisions; (iii) the available decision alternatives at each decision node; (iv) the information available to the adversary at each decision node; and (v) the utilities for the adversaries resulting from any sequence of events, it is possible to produce plausible predictions concerning the adversaries’ likely actions, ensuing outcomes, and consequences for each adversary.

Our methodological development refers extensively to the basic sequential defend-attack game, visualized as a bi-agent influence diagram in Fig. 1. This is a stochastic game of incomplete information in which all the actions and random events are observable after-the-fact, so it also features perfect information. The Defender’s nodes are shown in blue and those of the Attacker in red. The node Θ represents an uncertain outcome which is common to both adversaries and colored in both colors. The dashed arc between the Defender’s and Attacker’s decisions describes an information structure, indicating that the Attacker knows the De-

![Fig. 1. A bi-agent influence diagram depicting the sequential defend-attack game.](image-url)
fender’s decision when the Attacker (A, referred to as ‘he’) makes his decision.

Specifically, the Defender (D, referred to as ‘she’) first implements her defensive decision \(d \in D\). Next, the Attacker observes this defense and makes his decision \(a \in A\). Finally, the combination of these decisions affects the probabilities of possible outcomes at the chance node \(\Theta\). The realized outcome \(\theta = \Theta(a, d)\) is typically uncertain and thus there is uncertainty about the consequences \(c(d, a, \theta)\). Often, these consequences involve multiple attributes, such as casualties, material losses and monetary costs for both adversaries.

The Defender evaluates the consequences with her utility function \(u_D(c(d, a, \theta))\) and the Attacker with his utility function \(u_A(c(d, a, \theta))\). For brevity, these utilities are denoted by \(u_D(d, a, \theta)\) and \(u_A(d, a, \theta)\), respectively. In the adversarial setting, the goals and, thus also the utility functions, of the players are different and often opposite.

2.2. Bayesian Nash equilibrium solution

As an example, we first determine the Bayesian–Nash equilibrium for the sequential defend-attack game in Fig. 1. From the Defender’s perspective, the uncertainties the Defender faces about the Attacker are modeled through a probability distribution over the set of Attacker’s possible types \(\mathcal{T}_A\), defined as combinations of \(\mathcal{U}_A\), the set of Attacker’s possible utility functions, and \(\mathcal{F}_A\), the set of his possible probability estimates for the outcomes \(\theta\) as a result of decisions \(a, d\). Thus, realizations of the Attacker’s type are pairs of utility functions and probabilities \(\mathcal{T}_A = (u_A, p_A)\). The solution for the game is obtained as follows:

1. At the outcome node \(\Theta\), compute the Attacker’s expected utilities

\[
\psi_{u_A, p_A}(d, a) = \int_{\Theta} u_A(d, a, \theta) p_A(\theta | d, a) d\theta,
\]

for every \((u_A, p_A) \in \mathcal{U}_A \times \mathcal{P}_A\) and decisions \(a \in A\) and \(d \in D\).

2. At the Attacker’s decision node \(A\), compute the optimal attacks for the observed defense \(d\) using the Attacker’s beliefs and utilities

\[
\psi_{u_A, p_A}(d) = \max_{a \in A} \psi_{u_A, p_A}(d, a),
\]

and forecast the attack \(a\) through

\[
p_A(a | d) = \mathbb{P}(A^* (d) = a),
\]

while taking into account the probability \(\mathbb{P}(\mathcal{T}_A = (u_A, p_A))\).

3. At the Defender node \(D\), compute the optimal defense

\[
d^* = \arg \max_{d \in D} \int_{A} \psi_D(d, a) p_D(a | d) da,
\]

where the Defender’s expected utility is

\[
\psi_D(d, a) = \int_{\Theta} u_D(d, a, \theta) p_D(\theta | d, a) d\theta.
\]

Solving the Attacker’s decision problem is more straightforward, because the Attacker can observe the defense \(d\) before choosing his mode of attack \(a\).

3. Games of partial information

Bayesian Nash equilibrium is the most widely used solution concept for games of incomplete information. Its application assumes that every player solves the game using Bayesian approach, i.e., all players assign subjective probability distributions to the parameters they do not know (Harsanyi, 1967). In practice, this assumption can be problematic, because defining subjective probability distributions over the other player’s probability estimates and utilities, or equivalently their type, can pose challenges. It also assumes that all players are willing and able to specify these probability distributions.

In order to support adversarial risk analysis when well-defined probability distributions over players’ types cannot be elicited, we explore how a game between rational players can be analyzed without such distributions. By rational, we mean that the players seek to maximize their own expected utilities. We also assume that the players have some knowledge about their adversary. Specifically, they are assumed to know that the other player’s type, characterized by a combination of utilities and beliefs \((u, p)\), belongs to a subset of possible types \(\mathcal{T} \subseteq \mathcal{U} \times \mathcal{P}\). In what follows, this characterization based on set inclusion is referred to as partial information.

Using these assumptions, we revisit the Defend-Attack game in Fig. 1. The Defender knows that the Attacker’s type \((u_A, p_A) \in \mathcal{T}_A\). For a given defense \(d\), the attack \(a\) is said to dominate attack \(a'\), denoted by \(a \succeq_A a'\), if and only if

\[
\int_{\Theta} u_A(d, a, \theta) p_A(\theta | d, a) d\theta > \int_{\Theta} u_A(d, a', \theta) p_A(\theta | d, a') d\theta, \quad \forall (u_A, p_A) \in \mathcal{T}_A.
\]

In particular, this dominance relation helps identify the attacks \(a' \in A\) that the Attacker will not choose in response to the defense \(d \in D\). Because the Attacker, being a rational player, will not choose the attack \(a'\) if its expected utility for him is lower than that of \(a \in A\). Thus, partial information \(\mathcal{T}_A\) about the Attacker type defines a strict partial order (an irreflexive and transitive binary relation) over the set of possible attacks.

3.1. Partial preference information and stochastic dominance

Using partial information to derive the dominance relation (1) is quite general and subsumes several cases of stochastic dominance for deriving a partial preference order over random variables (Levy, 1992). Specifically, assuming that \(p_A = p\) so that the Attacker’s probability estimates are known by the Defender, have consequences \(c(d, a, \theta) \in \mathbb{R}\) and have the Attacker’s utility function \(u_A\) belong to the set of all increasing utility functions \(\mathbb{I}^+\), Eq. (1) becomes

\[
\int_{\Theta} u_A(d, a, \theta) p_A(\theta | d, a) d\theta > \int_{\Theta} u_A(d, a', \theta) p_A(\theta | d, a') d\theta, \quad \forall (u_A, p_A) \in \mathcal{T}_A.
\]

In other words, every expected utility maximizing Attacker with an increasing utility function prefers attack \(a\) over \(a'\). When attack alternatives are viewed as choices between random variables, this is equivalent to stating that \(a\) dominates \(a'\) in the sense of first degree stochastic dominance, denoted by \(a \succeq_{FS} a'\).

Similarly, if the Attacker is risk averse, then his utility function belongs to the set of all increasing concave utility functions and consequently his decisions can be analyzed with second order stochastic dominance. Conversely, if the Attacker is risk prone, then \(\mathcal{U}_A\) can be taken to be the set of all increasing convex utility functions. Different degrees of stochastic dominance can be used to describe how decision makers with different risk attitudes would rank decision alternatives resulting in uncertain outcomes.

If the consequences \(c\) involve multiple attributes \(c_i\), it may not be known how important the different attributes are relative to each other from the Attacker’s perspective. When \(\mathcal{U}_A\) is the set of additive utility functions with increasing utilities for each attribute, aggregated with some non-negative (standardized) weights, the following Pareto-type first-order stochastic dominance holds

\[
a \succeq_{FS} a' \iff p_A(c_i(d, a, \theta) \leq e) \leq p_A(c_i(d, a', \theta) \leq e), \forall i, \forall e.
\]
where the inequality is strict for some combination of consequences \(e\) and \(i\). While the assumption of additive multivariate utility functions does not always hold, the inaccuracies caused by its minor violations are often acceptable in practice (Keeney & von Winterfeldt, 2011) and can be rectified by restructuring the attributes. Note that Pareto dominance can be defined similarly for higher orders of stochastic dominance for real-valued attributes. It is also possible to construct more conclusive dominance relations, provided that partial information about the relative importance of the attributes can be obtained (See also: Liesiö, Mild, & Salo, 2008; Liesiö & Salo, 2012).

The construction of a stochastic dominance relation from a set of utility functions has been studied extensively; see, for example, Hadar and Russell (1969), Bawa (1975), Fishburn (1980), Kim (1998) and Shaked and Shanthikumar (2007). Thus, instead of focusing on the construction of dominance relations, we consider how they can be used in ARA.

3.2. Defense-Attack game with partial information about the Attacker

Using the basic sequential defend-attack game in Fig. 1 as an example, we analyse it as a game with partial information.

1. At the outcome node \(\Theta\), given decisions \(a\) and \(d\), analyze the expected utility for the Attacker for each \((a, p_a) \in T_A\)
\[
\psi^A_p(d, a) = \int_{\Theta} u_A(d, a, \theta) p_A(\theta|d, a) d\theta.
\]

2. As the Attacker can observe the defense \(d\) chosen by the Defender, the set of non-dominated attacks \(A^*(d)\) at the node \(A\) can be computed based on the dominance relation \(\psi^A_p(d, a) \geq \psi^A_p(d, a')\) for all \((d, a) \in D\) and \((d, a') \in D\) from (1) as
\[
A^*(d) = \{a : \exists a' : a' \geq \psi^A_p(d, a') \}.
\]

3. At node \(D\), based on the Defender's expected utility
\[
\psi_D(d, a) = \int_{\Theta} u_D(d, a, \theta) p_D(\theta|d, a) d\theta,
\]
compute the set \(D^*\) of non-dominated actions in \(D\), using the dominance relation
\[
d \geq d' \iff \psi_D(d, a) \geq \psi_D(d', a'), \forall a \in A^*(d), \forall a' \in A^*(d')
\]
where the inequality is strict for at least one pair of attacks \(a, a'\).

The key difference with the Bayesian analysis in Section 2.2 is that, rather than determining how likely the different actions of the Attacker are, the emphasis is on identifying what actions are plausible. The emphasis on this latter question is motivated by the fact that the Defender is ultimately interested not so much in what the Attacker will do as in maximizing her own expected utility.

If the Defender does not know the probability of the Attacker’s responses \(p_A(d|a)\), she cannot calculate her expected utility \(\psi_D(d)\) exactly. However, the Defender can determine which of the Attacker’s responses \(A^*(d)\) are possible so that they have a positive probability. The Defender can use this information to calculate an upper and a lower bound for her expected utility for each defense \(d\), i.e.,
\[
\psi_{D}^{\max}(d) = \max_{a \in A^*(d)} \psi_D(d, a) \quad \text{and} \quad \psi_{D}^{\min}(d) = \min_{a \in A^*(d)} \psi_D(d, a).
\]

These upper and lower bounds can be used to check dominance relations between alternative defenses, because
\[
d \geq d' \iff \psi_D(d, a) \geq \psi_D(d', a'), \forall a \in A^*(d), \forall a' \in A^*(d') \iff \psi_{D}^{\min}(d) \geq \psi_{D}^{\max}(d').
\]

This improves computational efficiency, because there is no need to compare the consequences for all possible responses \(a \in A^*(d)\) when determining \(D^*\). In some cases, these bounds can be determined analytically to further improve computational performance. If, for example, one of the non-dominated attacks \(a\) causes most harm to the Defender no matter what the Defender does (i.e., \(\forall d \in D : \exists a \in A^*(d)\) such that \(\psi_D(d, a) < \psi_D(d, a')\), \(\forall a' \in A^*(d)\), one need not compare all non-dominated attacks to establish the lower bound for \(\psi_D\).

3.3. Partial information about both players

Sometimes, it may be impractical or impossible to specify the Defender’s beliefs and preferences completely. This situation belongs to the realm of robust Bayesian analysis (Rios Insua & Ruggeri, 2012). It can be analyzed by extending the results of the preceding section by assuming that
\[
u_0(d, a, \theta) = \overline{u}_D, \quad p_0(\theta|d, a) = \overline{p}_D.
\]
for the specified sets \(\overline{U}_D, \overline{P}_D\) of possible utility functions and probability distributions that represent partial information about the Defender’s preferences and beliefs, respectively. These sets define the set \(T_D \subseteq U_D \times P_D\) representing the Defender’s possible types.

For comparing the Defender’s defence alternatives, we define the dominance relation \(\geq_{P,U}\)
\[
(d, a) \nexists_{P,U} (d', a') \iff \int_{\Theta} u_0(d, a, \theta) p_0(\theta|d, a) d\theta \
\geq \int_{\Theta} u_0(d', a', \theta) p_0(\theta|d', a') d\theta, \forall (u_0, p_0) \in T_D.
\]

where the inequality is strict for at least one combination \((u_0, p_0)\) in \(T_D\). For the Defender, this covers the cases of stochastic dominance in Section 3.2.

We now proceed as follows:

1. At the outcome node \(\Theta\), compute the Attacker’s expected utility for
\[
\psi_{A}^{U_P}(d, a) = \int_{\Theta} u_A(d, a, \theta) p_A(\theta|d, a) d\theta,
\]
for each \((a, p_a) \in T_A\) and \((a, d) \in A \times D\). and similarly for the Defender, for each feasible pair \((u_0, p_0)\) in \(T_D\).

2. At the Attacker’s decision node \(A\), compute the set of non-dominated attacks \(A^*(d)\) for the observed defense \(d\).

3. At node \(D\), compute the set \(D^*\) of non-dominated defenses in \(D\) on the dominance relation
\[
d \geq d' \iff (d, a) \nexists_{P,U} (d', a') \iff (d, a) \nexists_{P,U} (d', a') \iff (d, a) \nexists_{P,U} (d', a')
\]
where at least one of the inequalities in (5) for the binary relation \((d, a) \nexists_{P,U} (d', a')\) is strict.

The approach in Section 3.2 cannot be applied here, because the upper and lower bounds for the Defender’s expected utility cannot be calculated if the Defender’s utility function is not known.

This notwithstanding, for some sets of utility functions an analogous approach may be taken. For example, if the consequences \(c(d, a, \theta)\) are assessed with a single attribute and the Defender’s preferences for these consequences are monotonic, then these preferences can be modeled with first-order stochastic dominance. It is also possible to establish the upper and lower bounds for the cumulative distribution functions
\[
F_{<}^{\psi}(c(\theta'|d)) = \max_{a \in A} \int_{-\infty}^{\theta'} p_0(c(d, a, \theta)) d\theta
\]
\[
F_{<}^{\psi}(c(\theta'|d)) = \min_{a \in A} \int_{-\infty}^{\theta'} p_0(c(d, a, \theta)) d\theta.
\]
and to use first-order stochastic dominance based on the comparison of bounds to determine the non-dominated decision alternatives
\[ d \succeq_a^D d' \iff (d, a) \succeq_{P_{D_a}}^D (d', a'), \forall a \in A^*(d), \forall a' \in A^*(d') \]
\[ \implies F_{\min}^c(c(\theta^i | d)) \leq F_{\max}^c(c(\theta^i | d')), \forall \theta^i, \]
with strict inequality for some \( \theta^i \).

Similar methods can also be applied to examine preferences for higher orders of stochastic dominance or Pareto dominance. In the first case, one can compute the upper and lower bounds for the integral that is used for the comparison, whereas in the additive multi-dimensional Pareto case it is necessary to establish bounds for the marginal cumulative distribution functions of each of the attributes.

### 3.4. Decision rules

The approaches in Sections 3.2 and 3.3 seek to provide as conclusive results as possible based on the available information. However, if the specification of the adversaries' preferences and beliefs is very incomplete, the resulting sets of non-dominated defense and attack decisions may be too large to provide actionable decision support. This is a worthwhile result in and of itself, because it shows that the available information is insufficient for recommending a well-founded decision. If additional information about the players' types cannot be readily obtained, the set of recommended decisions can be narrowed down by introducing additional constraints. One can also apply decision criteria such as maximax, maximin or minimax regret from Bayesian robustness analysis (Rios Insua & Ruggeri, 2012). See also the approach presented by Mclay, Rothchild, and Guikema (2012), who consider robust optimization ideas in ARA contexts based on worst case scenarios.

For the Defender, the maximin decision rule for the set of non-dominated decisions is
\[ D^*_\maximin = \max_{dcD^*} \min_{a \in A^*(d)} \psi_{\theta}(d, a). \]

If the Defender's utility function is known, \( D^*_\maximin \) contains a single alternative (or multiple equally preferred alternatives) which can be determined using the upper and lower bounds on the expected utility from Eq. (4)
\[ D^*_\maximin = \max_{dcD^*} \psi_{\theta}^{\min}\min\psi(d). \]

Optimal decision sets for maximax and minimax regret can be constructed similarly.

As in Section 3.3, the set \( D^*_\maximin \) can be computed more efficiently if the Defender's preferences over the uncertain consequences fulfill first-order stochastic dominance. Then, the upper and lower bounds of the cumulative distribution functions from (7) can be employed to determine the non-dominated decision alternatives
\[ D^*_\maximin = \{d \in D^* : \exists d' \in D^* : F_c^{\max}(c(\theta | d)) > F_c^{\max}(c(\theta | d')), \forall \theta\}. \]

From the Defender's perspective, the upper bounds correspond to the worst possible combinations of the Attacker's and the Defender's preferences over consequences. The same approach can be applied to study other stochastic dominance relations.

In contrast to the use of decision rules in decision analysis, the Defender's choice between maximax, maximin and minimax regret decision rules may not reflect the Defender's risk attitude in the traditional sense as much as it reflects the Defender's aversion to the ambiguity associated with the Attacker's subsequent response. For example, the choice of the maximin decision rule limits the harm resulting from the Attacker's response to a minimum, whereas the minimax regret limits the downside variability in the Defender's expected utility. In some ARA problems, there could even be an ally instead of an Attacker, in which the Defender could choose the maximax decision rule to give the ally the opportunity to help her as much as possible.

### 3.5. Complex influence diagrams

Analyses based on partial information can be extended to more complex influence diagrams. In fact, the approach can be used to solve any regular multi-agent influence diagram in which the assumption of no forgetting holds. Regularity means that the influence diagram contains a directed path which traverses all decision nodes (regardless of which player they belong to) and thus defines a total order on them. The “no forgetting” assumption means that a player knows all the decisions and chance events that precede his/her current decision. Thus, such an influence diagram represents a sequential game of perfect information.

As shown by Shachter (1986) and Tatman and Shachter (1990), any regular influence diagram with no forgetting can be evaluated with a node elimination algorithm. Ortega, Rios, and Cano (2019) have extended this to bi-agent influence diagrams. A regular influence diagram can be solved with five graphical transformations:

1. Barren node elimination
2. Arc reversal between chance nodes
3. Chance node removal
4. Decision node removal
5. Value node removal

Barren node elimination removes non-utility nodes without children. The arc reversal transformation between chance nodes presented by Shachter (1986) is based on Bayes' rule and does not require any special considerations when dealing with partial information. The transformations for node removal, however, are more involved.

Fig. 2 shows the chance node removal operation. The cloud shaped nodes represent other parts of the influence diagram and can contain multiple decision and chance nodes as well as any number of arcs within themselves and between each other as long as the diagram remains regular. If a chance node has only children which are utility nodes belonging to different players, it can be removed by conditional expectation and the utility nodes inherit all the chance node's parents. In a multi-agent influence diagram, every utility node is associated with some player \( i \) with possible types \( T_i \subseteq U_i \times P_i \). As in (1), to remove the chance node \( X \) we compute a new partial order ranking the states of the new parent nodes \( A, B, \) and \( C \). That is, \( (a, b, c) \geq_{ABC} (a', b', c') \) if and only if
\[ \int_{X} u_i(b, c, x) p_i(x | a, b) dx \geq \int_{X} u_i(b', c', x) p_i(x | a', b') dx, \forall (u_i, p_i) \in T_i, \]
where the inequality is strict for at least one feasible pair of utility functions and probability distributions \( (u_i, p_i) \in T_i \). The partial preference order \( \geq_{ABC} \) is then used to form the new \( T_i' \subseteq U_i' \times P_i' \) for the new game represented by the modified influence diagram.

![Fig. 2. Chance node removal.](image-url)
This process is repeated for all the players whose utility nodes had $X$ as a parent.

Fig. 3 illustrates the decision node removal operation. If all the children nodes for the decision node $D$ for player $i$ are utility nodes so that none of them have parents which are also shared by $D$, such decision node can be removed by maximization, in which case the utility node belonging player $j$ inherits all the chance node's parents. (It is also possible that $i = j$.) As before, the players' possible types are represented by $\mathcal{T}_i \subseteq \mathcal{U}_i \times \mathcal{P}_i$ and $\mathcal{T}_j \subseteq \mathcal{U}_j \times \mathcal{P}_j$.

We first determine non-dominated decision alternatives of player $i$ at node $D$ similarly as in Eq. (3)

$$\mathcal{D}_i^1 (a, b, c) = \{ d : \exists d' : d' \mathrel{\geq_D} d \},$$

where $\mathrel{\geq_D}$ is derived from the utilities of player $i$. It is worth noting that if this player has no utility node as a child of $D$, then nothing is known about his decision and $\mathcal{D}_i^1 = \emptyset$. Utility node $U$ is then updated based on $\mathcal{D}_i^1 (a, b, c)$ similar to (6) in that

$$(a, b, c) \mathrel{\geq_{ABC}} (a', b', c') \iff$$

$$(d, c) \mathrel{\geq_{DC}} (d', c'), \quad \forall d \in \mathcal{D}_i^1 (a, b, c), \forall d' \in \mathcal{D}_i^1 (a, b, c),$$

where $\mathrel{\geq_{DC}}$ represents the partial preference order of player $j$ over states of $C$ and $D$. It is reduced to an expected utility comparison if the type $\mathcal{T}_j$ for player $j$ is known. The partial preference order $\mathrel{\geq_{ABC}}$ is then used to form the new $\mathcal{T}_j' \subseteq \mathcal{U}_j' \times \mathcal{P}_j'$ for the new game represented by the modified influence diagram. This process is repeated for all the players whose utility nodes have $D$ as a parent.

Sometimes it may be convenient to represent player’s utilities with several utility nodes. If the utility nodes share a parent node, it eventually becomes necessary to combine them to completely solve the influence diagram. Fig. 4 depicts how two utility nodes are combined into one and the new node inherits the parents of both. The partial preference relation describing the new utility node just has to be consistent with the removed ones

$$(a, b, c) \mathrel{\geq_{ABC}} (a', b', c') \iff$$

$$( (a, b) \mathrel{\geq_{AB}} (a', b') ) \land ( (b, c) \mathrel{\geq_{BC}} (b', c') ).$$

Utility nodes belonging to different players cannot be normally combined in this way. Still, this does not prevent solving the influence diagram, because decision and chance nodes can be removed even if they have multiple different players’ utility nodes as children.

With the last three graphical transformations now compatible with partial information, we can solve all sequential games of perfect information. The transformations can also help solve complex non-sequential games, but they cannot be used to eliminate decision nodes when an utility node has multiple decision nodes

parents, as is the case in Fig. 5. All decisions that do not lie on the same directed path need to be solved simultaneously, and depending on the partial preference order at the utility node $U$ and the number of decision nodes, this may be fairly straightforward or nearly impossible. For some preference orders it is possible to eliminate dominated pure strategies iteratively in order to reach an equilibrium solution (Börgers, 1994) For others, it is necessary to also consider mixed strategies (Perea, Peters, Schulteis, & Vermeulen, 2006). To our knowledge, non-sequential partial information games more complex than the one in Fig. 5 have not been studied.

4. Planning of countermeasures for unmanned aerial vehicles

We illustrate our methods for solving complex influence diagrams with a realistic case study from military planning. We examine a scenario in which the Defender seeks to protect her supply company from the Attacker’s reconnaissance activities. Specifically, the Attacker seeks to map the position of the company with UAVs. If the Attacker succeeds in this mapping activity, he can use either artillery or heavy rocket launchers against the Defender’s supply company. The following ARA is produced for the Defender who seeks to assess the cost-efficiency of UAV-countermeasures for investment planning.

4.1. Scenario description

The scenario is shown as a bi-agent influence diagram in Fig. 6. The Defender has deployed a supply company around the village of Tarttila, Fig. 7. The Defender seeks to protect the company from artillery fire and hence also from UAV reconnaissance as cost-efficiently as possible. Towards this end, she considers two different anti-UAV weapon systems, two different radar systems, and the option of improving camouflage. She also has to choose how many weapon systems to buy and where to place them.

The Attacker seeks to destroy or cripple the supply company by inflicting losses through artillery fire. The Attacker knows only the general area where the company is located. The Attacker can employ three types of UAVs for reconnoitering artillery targets. All types of UAVs can be equipped with one of two different sensor systems. Because the UAVs cannot send information back in real time, they must survive long enough to return to their base. The UAVs cannot change their flight paths based on what they observe.

The Attacker has several artillery and rocket launcher systems with unguided ammunition. After examining the information provided by the UAVs, the Attacker decides how to employ these systems.

The Defender does not know how many UAVs or artillery systems the Attacker has, or how much it would cost for the Attacker to use or lose them. Nor is the Attacker’s decision to use artillery or UAVs guided by these costs in the combat scenario. Overall, the Defender does not have complete information about the Attacker’s utilities.
4.2. Partial preference information

To keep this case study as realistic as possible, we use only as limited information about Attacker’s preferences as one could expect to have in an actual military conflict. The Attacker wants to maximize the damage to Defender’s equipment and personnel. At the same time he does not want to use ammunition unnecessarily for a given effect and prefers not losing UAVs. Because the Defender does not know what kind of UAV losses or ammunition costs the Attacker is willing to incur in order to cause to damage to the Defender, the Attacker’s preferences over outcomes are formulated through Pareto-type first-order stochastic dominance (Eq. (2)). Specifically, the Attacker is assumed to (i) minimize ammunition consumption and UAV losses, and (ii) maximize the damage to the Defender’s supply company. In addition, using Pareto dominance includes the assumption that the utilities for each of these attributes are additive and independent.

Because there can be a considerable delay between the Defender’s investment in countermeasures and the actual deployment of these countermeasures, it can be challenging to formulate a utility function which accurately reflects trade-offs between immediate costs and uncertain future casualties. Thus, in the initial analysis, Pareto dominance is also employed to characterize the Defender’s preferences for defense alternatives. Specifically, the Defender seeks to (i) minimize the losses to her supply company and (ii) maximize the amount of ammunition that the Attacker would have to use to cause such losses. The Defender also seeks to minimize the cost of her UAV countermeasures.

4.3. Artillery fire

Following the process described in Section 3.5, the first node to be eliminated from the influence diagram in Fig. 6 is Supply company losses from artillery fire. To eliminate the node, we calculated the conditional probabilities for equipment and personnel losses as a function of how the Attacker would aim his Artillery and how many shells or rockets he would fire. These probabilities were computed with the operation analysis software Sandis (Lappi, 2008).

We first chose 10 locations for the Defender’s units that the Attacker might be able to identify using his reconnaissance. These same locations were used as targets for the artillery. It was determined the Attacker would be unlikely to accurately identify what equipment and personnel the Defender has at each of these locations, so all locations were deemed equally attractive to the Attacker. As can be seen from Fig. 8, the effects of the artillery fire increase when the Attacker uses more ammunition or divides fire between more targets. Unsurprisingly, damage to equipment and personnel were practically perfectly correlated. With this information, we can eliminate the chance node and update preferences for both sides. The preferences about supply company casualties now become irrelevant, because no other node affects them, so they are removed. The Attacker’s preferences are updated and he wants to use as much ammunition as possible and spread it between as many locations as possible. The Defender, on the other hand, would prefer just the opposite.

The next node to be eliminated is the Attacker’s decision node about how to use artillery. This decision depends on how many targets have been discovered by the UAV reconnaissance. The Attacker wants to use as much ammunition as possible to inflict maximum casualties, but, at the same time, he wants to conserve ammunition. These objectives are so obviously in conflict that no decision alternative is going to be dominated based on them. Because the Attacker prefers to spread artillery fire between as many targets as possible, he will always prefer to have as many as possible targets to aim at. Thus, when the Attacker’s decision node is removed, he will no longer have preferences over aiming locations or ammunition consumption, but higher number of targets identified with UAV reconnaissance is now preferable. The Attacker also still wants to minimize UAV losses. The Defender wants to minimize the number of targets identified by the UAVs, maximize UAV losses, and minimize investment costs.

4.4. UAV reconnaissance

After eliminating the uncertain effects of the artillery fire and Attacker’s decisions concerning it, the influence diagram has been reduced to a Defend-Attack game of UAV-reconnaissance, Fig. 9. The decision alternatives that remain for the Defender and Attacker at the remaining decision nodes are given in Tables 1 and 2, respectively. Because the Attacker can observe the Defender’s decision, the Attacker’s non-dominated responses to the Defender’s decision are determined first.
We built a MATLAB simulation tool to estimate the effectiveness of UAV reconnaissance. The tool incorporates a radar model that computes the detection probability based on physical and technical properties of the UAVs and radars and a simple weapon model that automatically destroys any UAVs that are within effective weapon range and have been detected. The conditional probability distributions for the detecting different numbers of target points were estimated through Monte Carlo simulation of random UAV flight paths.

The simulations were carried out for all combinations of Defender's and Attacker's decisions, making it possible to compute the Attacker's non-dominated response(s) to the Defender's decisions and weather conditions. The Attacker's decisions were evaluated based on the use of Pareto dominance for the two main objectives, i.e., the Attacker prefers to lose as few UAVs as possible and find as many target points as possible. No assumptions were made about how important these two objective would be to the Attacker.

The final step is to examine what decisions can be optimal in maximizing the Defender’s expected utility. We did not elicit an exact utility function from the Defender, but we have a partial stochastic ordering based on the Defender’s attribute specific preferences, similar to Section 3.3. Solving the problem using Pareto dominance over costs and the number of detected targets lead to 1271 non-dominated defense portfolios for the Defender. This is fewer than the 7689 at the outset, but still too many to recommend a decision. One reason why there are so many non-dominated portfolios is that the Attacker’s response to the Defender’s countermeasures is uncertain. This leads to wide bounds for the probabilities of finding different numbers of targets, see
Because the Defender’s utility function is not fully specified, the maximin decision rule does not yield a single decision. However, this rule reduces the number of non-dominated decision portfolios to 30 of which most differ only in the placement of the weapon systems. There are only 11 different equipment combinations, shown in Table 3. Many of the less costly alternatives, like the one which ignores UAVs entirely, do not protect the supply company well, but are non-dominated due to their low cost.

The results show that, for instance, the more expensive laser weapon system should not be chosen and the more expensive new radar is worthwhile only if the Defender is willing to spend at least 320 units. Because there are only a few alternatives, it would be possible to present the Defender with a detailed analysis of the probabilities with which the targets are discovered and what the likely effects of artillery fire are; or to present a well-founded overall assessment of what the most cost-efficient countermeasures are (Kangaspunta, Liesiö, & Salo, 2012).

Computing the non-dominated decision alternatives for the Defender took around 10 minutes using a fairly typical laptop and custom MATLAB code that was not optimized for speed. This is orders of magnitude less time than it took to compute the conditional probability tables for the chance nodes, which took days for the artillery fire and hours for the UAV reconnaissance using the same computer. Calculating the conditional probabilities for the effects of artillery fire turned out unnecessary in the end, because they only affected the decision dominance in very predictable ways. Using Bayesian Nash equilibrium to solve the same problem would have actually required those conditional probabilities.

For more complex problems, the computation time for this kind of dominance-based analysis increases much in the same way as in Bayesian Nash equilibrium analysis, i.e., it grows exponentially with the number of parents and children at decision nodes. However, the number of conditional probabilities in the chance nodes grows just as fast. This means that in many practical applications, the burden involved in eliciting them is likely to overshadow computational difficulties in solving the actual game.

5. Conclusions

ARA is a promising approach to the management of risks in application areas such as security and defense, because in contrast to standard game theoretic approaches, it does not necessitate strong assumptions about common knowledge. Still, modeling the adversaries’ interlinked decision process can be challenging, given that in practice it may be exceedingly difficult or practically impossible to elicit complete information about the adversaries’ preferences and beliefs.

Motivated by this, we have proposed dominance concepts and associated computational methods for characterizing and synthesizing partial information in ARA. Specifically, we have considered several variants of partial information which reflect different types of partial information in the context of the sequential Defender-Attacker model. However, our approach can be readily extended to even more extensive ARA models which involve sequential decision making, by following the principles discussed in the context of more complex influence diagrams. The methods presented are
general enough that they can be used with either single or multi-attribute utilities.

We have also presented an illustrative case study on military planning in which the Defender seeks to protect its supply company from UAV surveillance. The salient elements of this case study are representative of the problems encountered in other ARA applications, for instance in the realm of cyber security. In particular, the proposed solution concepts for the analysis of partial information are likely to be useful when there are challenges in assessing the adversaries’ multi-attribute utility functions and probability estimates. For instance, it would be difficult to predict how a cyber criminal would weigh the risks of getting caught against potential gains.

ARA models with partial preference information can also be used to address problems which involve multiple decision makers with different objectives. For instance, in environmental decision making there are often multiple stakeholders whose utility functions can be difficult to elicit completely (Hämäläinen, 2015). In such settings, a partial order for the decision alternatives could be built by eliciting and synthesizing partial information from these stakeholders.

The partial information approach may help simplify complex ARA problems even if the adversaries’ preferences can be specified through utility functions. That is, because stochastic dominance does not require that the expected utilities are calculated exactly, there is no need to elicit complete probability information for the influence diagram either. As the case with artillery fire in the UAV case study shows, it may suffice to know the direction of change in the adversaries’ utilities in response to changes in the probability parameters.

Analyses based on partial information can also be applied to problems involving sequential decisions by multiple actors. Because any inaccuracies in estimated utilities will propagate and accumulate in ‘deep’ influence diagrams containing long paths between decision and chance nodes, it may be advisable to err on the side of caution and produce initial analyses based on partial information. Then, if the partial information approach does not narrow down decisions sufficiently, one can revert back to the more traditional approach, elicit the utility functions and repeat the analysis using sets of non-dominated decisions. This will still require fewer probability estimates than the specification of full parameters for the original problem.

Acknowledgements

We thank the research project’s advisory group, Esa Lappi, Markku Kujala, Sami Helle, Vesa Ryynä, and Tero Majamaa, from the Finnish Defence Forces for their contribution to the development of the case study and for their expert advice. We also thank the Finnish Defence Research Agency, and Bernt Åkesson especially, for providing access to the operations analysis tool Sandis.

Appendix A. Technical parameters in UAV simulations

Table 4 UAV parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Small UAV</th>
<th>Cheap UAV</th>
<th>Fast UAV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Radar cross-section</td>
<td>0.01 square meter</td>
<td>0.1 square meter</td>
<td>0.1 square meter</td>
</tr>
<tr>
<td>Speed</td>
<td>20 meter/second</td>
<td>30 meter/second</td>
<td>200 meter/second</td>
</tr>
<tr>
<td>Min altitude</td>
<td>20 meter</td>
<td>50 meter</td>
<td>50 meter</td>
</tr>
<tr>
<td>Max altitude</td>
<td>160 meter</td>
<td>500 meter</td>
<td>500 meter</td>
</tr>
<tr>
<td>Expensive sensor</td>
<td>1000 meter</td>
<td>1000 meter</td>
<td>1000 meter</td>
</tr>
<tr>
<td>Range</td>
<td>500 meter</td>
<td>500 meter</td>
<td>500 meter</td>
</tr>
</tbody>
</table>

Table 5 Radar parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Old radar</th>
<th>New radar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>60</td>
<td>100</td>
</tr>
<tr>
<td>Frequency</td>
<td>9.5 gigahertz</td>
<td>3.5 gigahertz</td>
</tr>
<tr>
<td>Peak power</td>
<td>80 Watts</td>
<td>60 Watts</td>
</tr>
<tr>
<td>Pulse duration</td>
<td>1 meter second</td>
<td>1 meter second</td>
</tr>
<tr>
<td>Net gain</td>
<td>15 decibels</td>
<td>15 decibels</td>
</tr>
<tr>
<td>Pulses integrated</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Probability of false alarm</td>
<td>1E-6</td>
<td>1E-6</td>
</tr>
<tr>
<td>Elevation angle</td>
<td>30</td>
<td>70</td>
</tr>
</tbody>
</table>

Table 6 Weapon parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Projectile weapon</th>
<th>Laser weapon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>110</td>
<td>160</td>
</tr>
<tr>
<td>Range</td>
<td>1000 meter</td>
<td>2000 meter</td>
</tr>
<tr>
<td>Limited by visibility</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

References


