Impact of biomimetic deception on AI underwater acoustic recognition

Paul Jézéquel[1,2], Franck Florin[1], Jean-Jacques Szkolnik[2], Abdel Boudraa[2]

1. Thales, France
2. IRENav (UR 3643), Ecole Navale/Arts & Métiers ParisTech, Brest, France.

Use case Identification

Underwater acoustic recognition is an essential area of underwater warfare. Underwater forces control their environment through passive monitoring, which allows them to recognise the actors present while remaining discreet themselves. For the operator, it consists of classifying the received sounds, that is to say, assigning them a potential threat level. The French Acoustic Interpretation and Recognition Center (CIRA) has recognised that the current context sees a considerable increase in the amount of data to be processed due to both increased maritime traffic and the performance of acoustic equipment. To cope with this and speed up the analysis of this massive data as well as the reaction time, the French Navy uses artificial intelligence (AI). AI is able to recognise non-threatening sounds and thus helps analysts sort the sounds so that they can focus their attention on useful signals with high added value (https://www.defense.gouv.fr/actualites/gagner-guerre-acoustique-grace-lintelligence-artificielle). In order to counter the proliferation of threats, analysts are equipping themselves with the best equipment and AI to help them recognise sounds that betray the presence of a threat.

Among these characteristic sounds, adverse sonar emissions and acoustic communication signals are highly recognisable signs that betray the presence of a threatening ship or drone swarm. In order to better resist the indiscretion produced by their own sonar or communication signals, several nations are interested in biomimetic deception in the field of underwater acoustic. It means masking a sonar emission or a communication signal as biological noise. In practice, the sonar emits a sound in the band of interest, very similar to that of, for example, a marine mammal. The interceptor who receives the emission is then deceived and is believed to face one of the many signals created by marine fauna. If the deception is successful, the automatic AI filters do not manage to properly characterise the perceived sound and the operator never accesses critical information. The intruder is never spotted. Such behaviour of AIs, unable to recognise the true from the false biological sound, poses a considerable threat to the recognition processing chain and the trust that operators can place in the machine. In the worst case, such an unfitness of the AI would cause significant backtracking, forcing the operator to process all acoustic signatures, thus losing considerable time and compromising the responsiveness of forces.

For passive monitoring, having an "artificial ear" capable of recognising biomimetic deception is therefore becoming an essential issue. Having an AI able to recognise a decoy or at least point out a possible deception would allow the operator to concentrate again on what is essential. To define such an artificial ear, we have chosen to review the most used techniques and signals and to analyse the use cases that are of potential operational interest.

Technical Approach

The work carried out as part of the NAIADE chair (NAvalisation de L'Intelligence Artificielle pour l'aide à la DEcision) in partnership between Thales and IRENAV (Institut de Recherche et d'Études Navales) is the subject of a CIFRE PhD supported by ANRT. Academic research conducted on the basis of available scientific literature aims at a technological maturity TRL3. The objective of this work is to study the impact of deception on the efficiency of the operator-AI association. The cases of detection sonars and acoustic communication devices are treated separately. If the use cases of biomimetic sonars may seem of limited operational interest, the use of biomimetic signals for acoustic communications could make it possible to mislead the alert detector in certain configurations and thus break the trust that humans place in AI, making new AI-based devices ineffective or even counterproductive.

The study highlights research laboratories and publication volumes according to their countries of origin. Chinese laboratories occupy a very significant part of the theme, but other nations are also concerned.

In the biomimetic approach, the choice of imitated marine species is a point of attention, since this choice must take into account the prevalence of the species and the interest of the frequency band used for an effective operational use. The study highlights that the most studied species are studied less for practical reasons of efficiency but rather for the availability of important public data.

There are many decoying techniques that must be distinguished according to the type of intended use (detection or communication) and the nature of the biological vocalisations used.

If we do not address in detail the physical means of achieving the decoy, we show, however, that it is necessary to take into account the constraints related to transducer technologies and sound wave propagation.

Moreover, the work addresses the issue of measuring the effectiveness of deception. If the available open scientific literature is interested in the ability of devices to deceive AI, the actual measurement of this deceptive capacity remains poorly treated and the proposed evaluation methods are unconvincing.

Thus, by analysing the different technologies published for acoustic biomimetic deception, we show that the subject is far from being a mere curiosity, but it shows a confirmed operational interest in taking into account AI in acoustic recognition processing.

The study must continue by analysing the methods and possible countermeasures in a few cases of interest for operational applications.

Impact du leurrage biomimétique en reconnaissance acoustique sous-marine

Paul Jézéquel[1,2], Franck Florin[1], Jean-Jacques Szkolnik[2], Abdel Boudraa[2]

1. Thales, France
2. IRENav (UR 3643), Ecole Navale/Arts & Métiers ParisTech, Brest, France.

Identification des cas d'usages

La reconnaissance acoustique sous-marine (ASM) est un domaine essentiel de la lutte sous la mer. Les forces sous-marines maitrisent leur environnement par l'écoute passive qui leur permet de reconnaitre les acteurs présents tout en restant elles-mêmes discrètes. Pour l'opérateur, il s'agit de classifier les sons reçus, c'est-à-dire leur attribuer un niveau de menace potentielle. Le centre d'interprétation et de reconnaissance acoustique (CIRA) a reconnu que le contexte actuel voit un accroissement considérable de la quantité de données à traiter en raison à la fois de l'augmentation du trafic maritime et de l'accroissement de la performance des équipements acoustiques. Pour y faire face et accélérer le temps d'analyse de ces données massives ainsi que le temps de réaction, la Marine a recours à l'intelligence artificielle (IA). L'IA est en mesure de reconnaitre les sons non menaçants et ainsi aider les analystes à trier les sons afin qu'ils portent leur attention sur les signaux utiles à forte valeur ajoutée. (https://www.defense.gouv.fr/actualites/gagner-guerre-acoustique-grace-lintelligence-artificielle). Ainsi pour contrer la prolifération des menaces, les analystes s'équipent des meilleurs équipements et de l'IA pour les aider à reconnaitre les sons qui trahissent la présence d'une menace.

Parmi ces sons caractéristiques, les émissions sonar adverses et les signaux de communications acoustiques sont des signes très repérables qui trahissent la présence d'un bâtiment ou d'une flottille de drones menaçants. Afin de mieux résister à l'indiscrétion produite par leurs propres signaux sonar ou de communication, plusieurs nations s'intéressent au leurrage biomimétique dans le domaine de l'ASM. Il s'agit de maquiller une émission sonar ou un signal de communication en bruit biologique. En pratique le sonar émet un son dans la bande d'intérêt, très similaire à celui, par exemple, d'un mammifère marin. L'intercepteur qui reçoit l'émission est alors leurré et croit faire face à l'un des nombreux signaux créés par la faune marine. Si le maquillage est réussi, les filtres automatiques de l'IA ne parviennent pas à caractériser convenablement le son perçu et l'opérateur n'accède jamais à l'information critique. L'intrus n'est jamais repéré. Un tel comportement des IA, incapables de reconnaitre le vrai du faux son biologique, fait peser une menace considérable sur la chaine de traitement de reconnaissance et la confiance que les opérateurs peuvent accorder à la machine. Dans le pire des cas, une telle inaptitude de l'IA provoquerait un retour en arrière significatif, obligeant l'opérateur à traiter toutes les signatures acoustiques, perdant ainsi un temps considérable et compromettant la réactivité des forces.

Pour l'écoute passive, disposer d'une « oreille artificielle » capable de reconnaitre le leurrage biomimétique devient donc un enjeu essentiel. Disposer d'une IA en mesure de reconnaitre un leurre ou au moins de signaler un leurrage possible, permettrait à l'opérateur de se concentrer à nouveau sur l'essentiel. Pour définir une telle oreille artificielle, on a choisi de passer en revue les techniques et les signaux de leurrage les plus usités et d'analyser les cas d'usage qui présentent un intérêt opérationnel potentiel.

Approche technique

Les travaux menés dans le cadre de la chaire NAIADE (NAvalisation de L'Intelligence Artificielle pour l'aide à la DEcision) en partenariat entre Thales et l'IRENAV (Institut de Recherche et d'Etude Navales) font l'objet d'une thèse CIFRE soutenue par l'ANRT. Les recherches académiques menées sur la base de la littérature scientifique disponible, visent une maturité technologique TRL3. L'objectif de ces travaux est l'étude de l'impact du leurrage sur l'efficacité du binôme opérateur-IA. On traite séparément les cas des sonars de détection et ceux des dispositifs de communication acoustiques. Si les cas d'emploi des sonars biomimétiques peuvent sembler d'un intérêt opérationnel restreint, l'usage de signaux biomimétiques pour les communications acoustiques pourrait permettre de leurrer le détecteur d'alerte dans certaines configurations et ainsi briser la confiance que l'humain accorde à l'IA, rendant les nouveaux dispositifs à bases d'IA inefficaces voire contre-productifs.

L'étude met en évidence les laboratoires de recherche et les volumes de publications en fonction de leurs pays d'origine. Les laboratoires chinois occupent une part très significative de la thématique, mais d'autres nations sont également concernées.

Dans l'approche biomimétique, le choix des espèces marines imitées est un point d'attention puisque ce choix doit tenir compte de la prévalence de l'espèce et de l'intérêt de la bande de fréquences utilisée pour un usage opérationnel efficace. L'étude met en évidence que les espèces les plus étudiées le sont moins pour des raisons pratiques d'efficacité que pour la disponibilité de données publiques importantes.

Les techniques de leurrage sont multiples et doivent être distinguées en fonction du type d'utilisation visée (détection ou communication) et en fonction de la nature des vocalises biologiques utilisées.

Si l'on n'aborde pas en détail les moyens physiques de réalisation du leurrage, on montre toutefois qu'il est nécessaire de prendre en compte les contraintes liées aux technologies de transducteurs et à la propagation des ondes sonores.

Par ailleurs, les travaux abordent la question de la mesure de l'efficacité du leurrage. Si la littérature scientifique ouverte disponible s'intéresse à l'aptitude des dispositifs à tromper des IA, la mesure réelle de cette capacité de leurrage reste peu traitée et les méthodes d'évaluation proposées peu convaincantes.

Ainsi en analysant les différentes technologies publiées pour le leurrage biomimétique acoustique, on montre que le sujet est loin d'être une simple curiosité, mais témoigne d'un intérêt opérationnel certain pour la prise en compte des IA dans les traitements de reconnaissance acoustique.

L'étude doit se poursuivre en analysant les méthodes et les contre-mesures possibles dans quelques cas de leurrage d'intérêt pour les applications opérationnelles.