Proceedings of the Thirtieth International Florida Artificial Intelligence Research Society Conference

Cognitive Adaptive Learning, Classification, and Response for Communications Threats (CALCR): A Case-Based Reasoning Approach

Elizabeth Whitaker and **Ethan Trewhitt**
Georgia Tech Research Institute, Atlanta, GA
{elizabeth.whitaker, ethan.trewhitt}@gtri.gatech.edu

David Rosenbluth
Lockheed Martin Advanced Technology Laboratories, Cherry Hill, NJ
david.rosenbluth@lmco.com

Abstract

The Cognitive Adaptive Learning Classification and Response for Communications Threats system, (CALCR) uses a case-based reasoning (CBR) and case-based learning (CBL) approach to address issues encountered in a contested RF communications environment. CALCR was the result of a research project that explored new approaches to understanding communications threats and responding with appropriate countermeasures. Modern communications threats may be modified from existing systems, or may be completely new systems, and CALCR enables a response to these unknown or unanticipated threats. CALCR integrates existing properties of CBR, along with several innovations, making it ideal for this problem: the ability for a case library to be extended through CBL as new conditions are encountered; the robustness of CBR in situations where there is missing data, which CALCR addresses with an advanced intelligent similarity measure; the ability to detect classes unknown to the case library through the use of a confidence measure; and the ability to provide a best-attempt solution, when multiple threat classes are matched, through the use of a new approach called the taxonomy reasoner.

Introduction

Modern communications threats can be daunting for countermeasure systems due to the difficulty in responding to unexpected situations. Communications threats in this research refer to radio transmissions (along with the associated transmitters and channels) from sources which mean to do harm to the given entity. The Cognitive Adaptive Learning Classification and Response for Communications Threats (CALCR) uses a case-based reasoning (CBR) and case-based learning (CBL) approach to recommend countermeasures that respond to a communications threat. The approach must be able to recognize whether a threat is already represented in the system and to learn a new representation otherwise.

This application of case-based reasoning builds upon the body of knowledge that precedes it. It uses two different styles of CBR: one for classifying the threat and one for synthesizing a countermeasure. These use two different case-libraries to solve these two types of problems as described in Leake and Kinley (1998), who integrated multiple case-based reasoning tasks into a case-based learning problem. For countermeasure synthesis in CALCR, a small set of rules is used to adapt the countermeasures of the new problem to match the specific transmitter, transmission, channel configuration that is observed in the incoming threat. This adaptation approach has been used since the earliest days of CBR (detailed in Marling et. al. 2002).

CALCR is part of a larger architecture that integrated multiple learning and reasoning approaches through a centralized integrating component called the Cognitive Map. CBR (Kolodner 1993 and Watson 1997) is applied to classify signals and to synthesize and recommend appropriate responses to mitigate a wireless communications threat. We introduce our multi-stage approach to classifying signals and synthesizing countermeasures through adaptation (Whitaker & Simpson 2004). We discuss a taxonomy reasoner, a new approach, which is used in situations where the exact class is not represented in the case library. In this case, with the help of the Taxonomy Reasoner, CALCR can help synthesize the countermeasure by using knowledge about the shared or inherited features that may affect multiple classes. CALCR includes a technique for using the confidence measure to recognize when an observed class is not represented in the case library and the use of that information for case-based learning. Our project included a design for CBL in the countermeasures synthesis mode using Battle Damage Assessment (BDA). Although this feature was not tested in the project, we discuss the design.

CALCR provides: the ability for the case library to be extended through case-based learning as new conditions are encountered, robustness against missing data, the ability to detect classes that are not represented in the case library through the use of a confidence measure, and the ability to provide a workable solution when the system does not have enough information for an ideal solution through the use of a new approach called a taxonomy reasoner.

The CALCR prototypes are integrated into a larger intelligent learning and processing system resulting in a hybrid learning system (Zhang et. al. 2009) interacting via the Cognitive Map to combine results. In the context of a cognitive electronic warfare (EW) system, the information captured in the Cognitive Map combines prior radio frequency (RF) sensor data with *a priori* semantic/relational knowledge about communications in general, into a geographic picture of entities in the communications environment, their characteristics, and their relations (Rosenbluth et. al. 2012).

Case-Based Reasoning for CALCR

Case-based reasoning (CBR) consists of solving new problems by reasoning about past experiences (Kolodner 1993). Experiences are captured and stored as a collection of cases stored in a case library. Each of these cases contains a past problem and the associated solution and is indexed by a set of features which characterize the case. Solving new problems involves identifying relevant cases from the case library using a similarity measure and reusing or adapting their solutions to solve the problem at hand using specialized domain-specific adaptation knowledge.

Table 1. CALCR Case Features

Transmitter	Transmission	Channel
Latitude	Number of Antennas	Center Freq.
Longitude	Onset Time	Bandwidth
Line of Bearing	Offset Time	Capacity
Protocol	Duration	Occupancy
Duty Cycle	Modulation Type	Throughput
Transmit Power	Number of Channels	Duplex
		Switching
		Network
		Multiuser

A high-level view of the case-structure is provided in Table 1. The features fall into three categories: features of the transmitter, features of the transmission, and features of the channel through which the transmission occurs.

The basic case-based reasoning system in CALCR works as follows:

1. The CBR component is passed objects that list the attributes or features of detected threats, which have been added to the Cognitive Map. The new problem is structured into a format compatible with the case structure by the Feature Extractor, which takes the information from the objects and formats it into a target case that will be compared with cases in the case library.
2. The Retrieval process compares the target case with cases in the case library to select one or more cases that most closely resemble the target case, using a similarity measure for this comparison. Case-based reasoning relies on the assumption that if two problems are "close" in the problem space then their solutions are likely to be "close" in the solution space (Hüllermeier 2000).
3. If a similar case is found in the case library, the solution to the selected case is transformed, or "adapted", to solve the new problem represented by the target case. The function of the *Adaptation* module in a CBR system is dependent on domain knowledge of the problem space. For adaptation in the countermeasures stage of CALCR, (described later) a small set of rules were provided by the communications domain experts.

A similarity measure is based on the feature space distance between a case in the case library and the target case. It defines the difference between cases as characterized by the case feature set. Over the course of this project we experimented with and iterated on the similarity measure in the communications signal CBR feature space. The communications domain required a flexible approach that includes a weighted Euclidean feature distance. The $similarity_i$ = 1 – *normalized distance*. CALCR compares the target case with every case in the case library and select one or more "nearest neighbors." CALCR tuning starts with a set of weights recommended by a domain expert, but those weights will likely be refined through experimentation.

We modified our Euclidean similarity measure for features with special characteristics. One example is a feature in which inequality between cases is important but not the magnitude of the inequality. For such features a Boolean similarity measure B will provide a "1" to the similarity measure if a feature in the target case T_i matches the feature F_i in the comparison case within a threshold t_i. It will provide a 0 to the similarity measure otherwise.

$$similarity_i = \frac{\sum\left(B(F_i, T_i, t_i)\right)}{n}$$

Where $B(F_i, T_i, t_i) = \begin{Bmatrix} 1 & |T_i - F_i| \le t_i \\ 0 & otherwise \end{Bmatrix}$

Number of Channels is one such feature: if two cases have mismatched channel counts, it is not useful to compare the difference between the two channel counts.

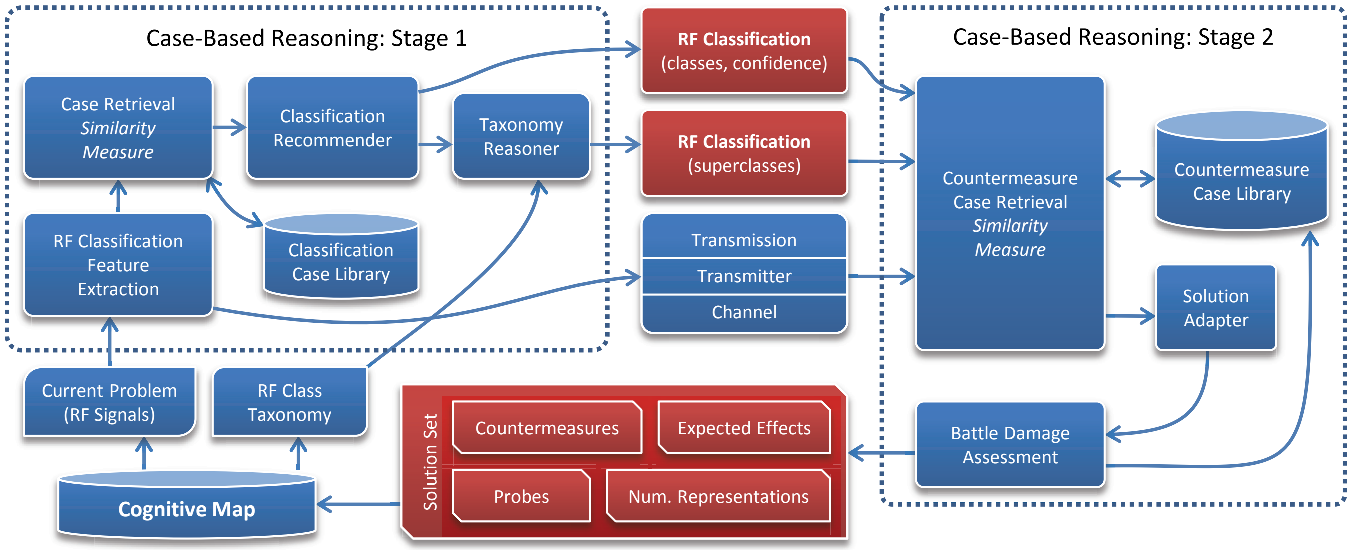

Figure 1. CBR Performance Mode

Two-Stage Process: Case Bases to Represent the Communications EW Problem

CALCR included a two-stage process with multiple case libraries. The first stage classifies the target case as an emitter class, while the second stage performs uses both the original RF features and the derived class (from the first stage) to select and configure an appropriate countermeasure. Figure 1 shows this process.

Stage 1 (Classifying a signal)

1. A signal is received by the system
2. Objects are created representing the features of the signal's transmitters, transmissions, and channels.
3. The characterization is passed to the CBR module through the Cognitive Map.
4. The CBR *Feature Extractor* is applied to produce a target case, generating a set of statistical features of the transmitters, transmissions, and channels of the incoming signal.
5. The most similar cases are identified.
6. The Taxonomy Reasoner combines the matching characteristics of conflicting threat classes, when appropriate, to enable an effective partial match.

Stage 2 (Synthesizing countermeasures)

1. The new threat class is passed to the CBR *Countermeasures* module as the stage 2 target case.
2. The most similar cases are retrieved.
3. Adaptation is applied to transform the countermeasure settings in the retrieved case to the target case.
4. Appropriate countermeasure parameters are synthesized using the rules engine previously created by domain experts.
5. An explanation of the reasoning done to produce the countermeasures is provided for human consumption.
6. Any input to modify the countermeasure can be contributed by a human at this point.

Reusing Cases to Classify RF Signals

When the case-based reasoner is being used in a classification problem (one of the uses for CBR in this project), retrieval will include the k nearest neighbors, which provides more robustness than retrieving a single best match. This method provides a set of potential classifications and associates a confidence value with each. The CBR component is passed objects (through subscription) that list the attributes or features of detected threats which were produced by or compiled by the cognitive map. Information from the object is structured into a format compatible with the case structure by the CBR *Feature Generator.*

Based on the case to be classified and a similarity function, the *Retrieval* module calculates the relevance (similarity) of each case in the case base, then returns the k most relevant cases. For $k = 8$, CALCR measures the distance in feature space of each case in the case base from the case to be classified, then returns the eight nearest cases (nearest neighbors in feature space). In a classification problem we will not "adapt" the solution but rather select or recommend the problem class, based on the classes of the k nearest neighbors. The *Recommender* module receives the most relevant cases as input, and based on a predefined function, assigns each possible classification a confidence value. CALCR defines the confidence for a classification as the sum of the similarities of each of the k nearest neighbors with that classification, divided by the total sum of the similarities for the k nearest neighbors. This allows the CBR component to benefit from the combined information of multiple cases without prior generalization.

Taxonomy Reasoner

If the CBR module is not able to classify a signal with a high confidence, it will use the signal taxonomy to provide further knowledge to guide the system. This situation will occur if the *k* nearest neighbors are from two or more classes and the sum of confidence levels across each class do not allow for a definitive classification. The CBR module will use the *Taxonomy Reasoner* to reason about common ancestry of the resulting set of classes. It will use associated confidence levels to determine with a higher certainty what superclass (next higher node in the taxonomy tree) the signal belongs to. See Figure 2. The CBR component can report the candidate superclasses and associated confidence levels to be included in the published data object provided to the Cognitive Map, which may allow downstream reasoning processes to perform based on the shared characteristics of the superclass without being able to distinguish from among the threat classes contained within it.

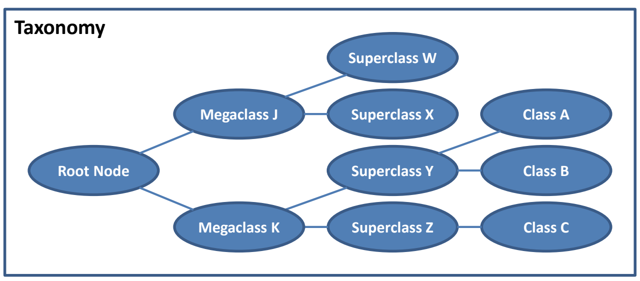

Figure 2. Sample taxonomy of classes

Reusing Cases to Generate Countermeasures

For CBR countermeasure synthesis, the *Retrieval* module selects one or more countermeasure cases from its case library. Each case contains a countermeasure identifier (i.e., method name) and a set of parameter assignments. The *Adaptation* module uses a set of rules to transform the countermeasure associated with each of the selected cases into an adapted countermeasure to be proposed for the target case. The rules are written as a function of the features of the selected cases, their countermeasure solutions, and the features of the target case. The adapted countermeasures will be passed to other components in the hybrid reasoning system, through the Cognitive Map, for evaluation and selection. The adaptation module's rule set is built from knowledge provided by communications signals experts. As the system is tested with simulated data, then real-world data, adaptation rules are updated by domain experts to adjust performance based on those results.

Conclusion

The CALCR project designed, prototyped, integrated and tested several aspects of case-based reasoning and learning applied to representing, characterizing and countering wireless communications threats. We developed and applied an approach to identifying unknown threats through the use of confidence measures. CALCR introduced the Taxonomy Reasoner to allow for best available solutions when more precise information is not available. A flexible approach to selecting the appropriate similarity measure was developed to deal with known challenges in the domain. An approach was designed to apply the results of battle damage assessment to the learning of new cases. CALCR was integrated into a hybrid reasoning system through a cognitive map for a more robust approach to characterizing and countering communications threats. The design produced for CALCR can be reapplied and integrated into a number of related military applications. Although CALCR underwent significant testing as part of the research prototype integration, next steps in moving toward a piloted integration system will include a major evaluation and parameter tuning effort.

References

Hüllermeier, E. (2000, August). Similarity-based inference as evidential reasoning. In Proceedings of the 14th European Conference on Artificial Intelligence (pp. 55-59). IOS Press.

Kolodner, J. L. (1993). Case-Based Reasoning. Morgan Kaufmann.

Leake, D. B., and Kinley, A. 1998. Integrating CBR Components within a Case-Based Planner. In Case-Based Reasoning Integrations: Papers from the 1998 Workshop, 80–84. Menlo Park, Calif.: AAAI Press.

Marling, C., Sqalli, M., Rissland, E., Muñoz-Avila, H., & Aha, D. (2002). Case-based reasoning integrations. AI magazine, 23(1), 69.

Rosenbluth, D., Dorsey, D., Tilghman, P., Byron, J., Whitaker, E., Trewhitt, E., Sardana, V., and Olivieri, M. (2012) Cognitive Representations of Communications for Electronic Warfare. MILCOM 2012.

Watson, I. (1997). Applying Case-Based Reasoning: Techniques for Enterprise Systems, Morgan Kaufmann, San Francisco.

Whitaker, E., & Simpson, R. (2004). Case-Based Reasoning in Support of Intelligence Analysis. Proceedings of 17th Annual FLAIRS Conference. Miami: AAAI Press.

Zhang, X. S.; Shrestha, B.; Yoon, S.; Kambhampati, S.; DiBona, P.; Guo, J. K.; McFarlane, D.; Hofmann, M. O.; Whitebread, K.; Appling, D. S.; Whitaker, E. T.; Trewhitt, E. B.; Ding, L.; Michaelis, J. R.; McGuinness, D. L.; Hendler, J. A.; Doppa, J. R.; Parker, C.; Dietterich, T. G.; Tadepalli, P.; Wong, W.; Green, D.; Rebguns, A.; Spears, D.; Kuter, U.; Levine, G.; DeJong, G.; MacTavish, R. L.; Ontañón, S.; Radhakrishnan, J.; Ram, A.; Mostafa, H.; Zafar, H.; Zhang, C.; Corkill, D.; Lesser, V.; Song, Z. (2012). An Ensemble Architecture for Learning Complex Problem-Solving Techniques from Demonstration. ACM Transactions on Intelligent Systems and Technology (TIST), 3(4).