R4-B.3: Advanced Automated Target Recognition (ATR) in Security Imaging

I. PARTICIPANTS

Faculty/Staff			
Name	**Title**	**Institution**	**Email**
Venkatesh Saligrama	PI	BU	srv@bu.edu
David Castañón	Co-PI	BU	dac@bu.edu
Joe Wang	Post-doc	BU	joewang@bu.edu
Ziming Zhang	Post-doc	BU	zzhang14@bu.edu
Graduate, Undergraduate and REU Students			
Name	**Degree Pursued**	**Institution**	**Month/Year of Graduation**
Greg Castañón	PhD	BU	5/2016

II. PROJECT DESCRIPTION

Core funding for this project ends in Year 3 per the outcome of the Biennial Review process.

A. Project Overview

We propose algorithms based on a hierarchical network of classifiers. This is critical both in portal systems, where high throughput requires significant automated decision support, and in standoff systems where the proliferation of multimodal data can overwhelm human interpretation.

Specifically, this project will leverage existing sensors, imaging modalities, and explosive detection algorithms. Some modalities, such as Active Millimeter Wave (AMMW) and Human Inspection, can be time-consuming. To improve detection performance and maintain high-throughputs, the proposed scheme will selectively route subjects sequentially through different stages. Subjects that do not pose threats exit the system early. In our preliminary experiments involving several benchmark datasets, we have shown that on average our scheme can improve throughput by as much as 50% without sacrificing detection performance. We have also conducted experiments with AMMW, Infrared and Passive Millimeter Wave (PMMW) modalities. For this scenario in our proposed scheme, we can show that with 47% AMMW utilization, namely, on 47% of selectively chosen subjects, we can match the detection rate when AMMW is used on all of the subjects. Since AMMW is far more time-consuming than Infra-Red (IR) it follows that our throughput gains can be significant.

The suite of new algorithms will improve effectiveness in the screening of people in airports, which is of significant interest to TSA. Our fundamental assumption is that it is too slow or costly to collect full sensor data on every object of interest, either for training, or during real-time operation. Thus, it is important to develop technologies that identify the right set of information to collect on individuals automatically, based on the most recent collected information.

The new algorithms will also impact standoff detection algorithms for suicide bombers, which is of interest to other agencies within DoD and the State Department. The efforts are aimed at developing a robust surveillance system for pervasive and persistent detection capability. Improved Automatic Target Recognition (ATR) concepts for Advanced Imaging Technology (AIT) is of particular interest to mm-wave and X-ray backscatter vendors. Our goal is to perform standoff detection of concealed explosives at low false alarm probability and near certain probability of detection.

The long-range impact of this research will be the development of adaptive, high throughput risk-based screening algorithms for different combinations of sensing modalities that exhibit improved sensitivity/specificity over conventional approaches.

B. Biennial Review Results and Related Actions to Address

The project had high technical ratings, but the project also had weaknesses, including the lack of specific transition pathways, milestones, and approaches for evaluation of competing methods. As such, the project was not recommended for continuation in Year 4.

C. State of the Art and Technical Approach

Conceptually, our work is closely related to Xu et al. [1,2] and Kusner et al. [3], who introduce Cost-Sensitive Trees of Classifiers (CSTC) and Approximately Submodular Trees of Classifiers (ASTC), respectively, to reducing test time costs. Like our effort, they propose a global Empirical Risk Minimization (ERM) problem. They solve for the tree structure, internal decision rules, and leaf classifiers jointly using alternative minimization techniques. Recently, Kusner et al. [3] proposed Approximately Submodular Trees of Classifiers (ASTC), a variation of CSTC which provides robust performance with significantly reduced training time and greedy approximation, respectively. Additionally, Nan et al. [4] proposed random forests to efficiently learn budgeted systems using greedy approximation over large data sets.

The subject of this project is broadly related to other adaptive methods in the literature. Generative methods [5-8] pose the problem as a partially observed markov decision process (POMDP), learn conditional probability models, and myopically select feature based information gain of unknown features. Markov Decision Process (MDP) based methods [8-11] encode current observations as state; unused features as action space; and formulate various reward functions to account for classification error and costs. He et al. [10] apply imitation learning of a greedy policy with a single classification step as actions. Dulac-Arnold et al. [9] and Karayev et al. [8] apply reinforcement learning to solve this MDP. Benbouzid et al. [11] propose classifier cascades with an additional skip action within an MDP framework. Nan et al. [4] consider a nearest neighbor approach to feature selection, with confidence driven by margin magnitude.

C.1. Hierarchical network of classifiers for high-throughput screening

Our work is closely related to the prediction time active feature acquisition (AFA) approach in the area of cost-sensitive learning. Our objective is to make sequential decisions about whether or not to acquire a new feature to improve prediction accuracy. Figure 1 (on the next page) illustrates some of the main concepts in this context. An individual, or their baggage, could either be inspected by an imaging technique such as X-Ray or Active Millimeter Wave, or inspected by a human. Some of these inspections are time-consuming, leading to low throughput. We can view the suite of sensors as a network and sequentially determine which object must be routed through what sensor. There are cases where an object must be flagged for complete human inspection while there are other cases that may only require X-ray. We hope to learn a policy that will adaptively determine which sensors to utilize for an object. In this way we propose to improve the average throughput.

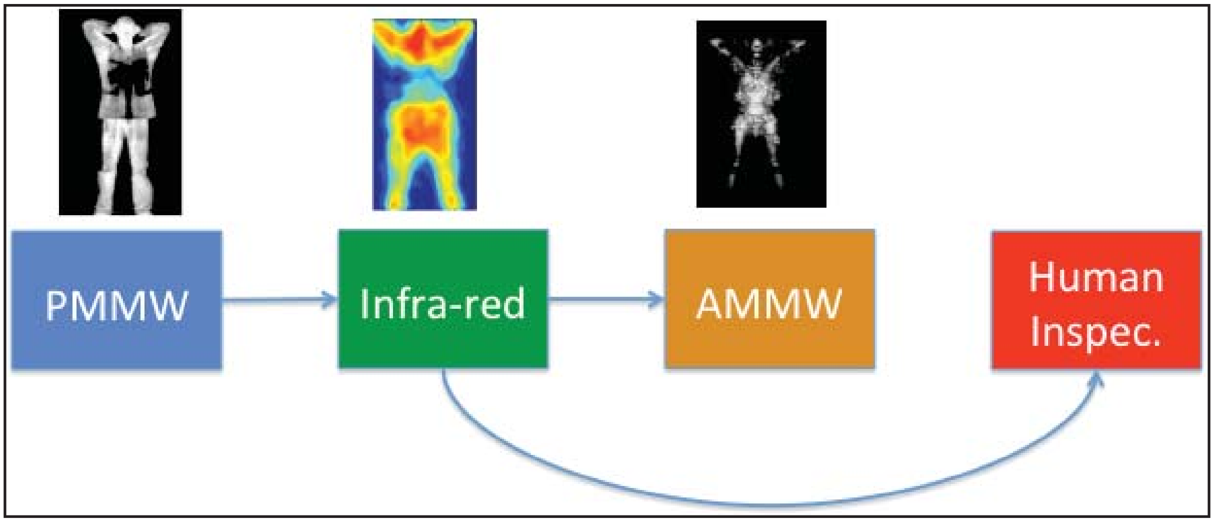


Figure 1: Proposed method illustrates a hierarchical network of classifiers for high-throughput screening for checkpoint screening. Some modalities such as AMMW and Human Inspection can be time-consuming. To improve detection performance at high-throughputs, the proposed scheme routes subjects sequentially through different stages. Subjects who do not pose threats exit the system early such as after an IR –based diagnosis.

There is extensive literature on adaptive methods for sensor selection for reducing test-time costs. It arguably originated with detection cascades, a popular method in reducing computation cost in object detection for cases with highly skewed class imbalance and generic features. Computationally cheap features are used at first to filter out negative examples and more expensive features are used in later stages. Our technical approach is closely related to our earlier work [12,13]. This earlier work is based on minimizing the Empirical Risk. In this context, detection cascades, classifier cascades and classification trees have been developed to handle balanced and/or multiclass scenarios. Trapeznikov et al. [12] proposed a similar training scheme on cascades. [12] utilizes simple decision functions for different nodes of the cascade and learns these decision rules by means of alternating optimization. Here we extend these approaches and study the problem of reducing test-time acquisition costs in classification systems. Our goal is to learn decision rules that adaptively select sensors for each example as necessary to make a confident prediction. We model our system as a directed acyclic graph (DAG) where internal nodes correspond to sensor subsets, and decision functions at each node choose whether to acquire a new sensor or classify using the available measurements. This problem can be posed as an empirical risk minimization over training data. Rather than jointly optimizing such a highly coupled and non-convex problem over all decision nodes, we propose an efficient algorithm motivated by dynamic programming. We learn node policies in the DAG by reducing the global objective to a series of cost sensitive learning problems. Our approach is computationally efficient and has proven guarantees of convergence to the optimal system for a fixed architecture. In addition, we present an extension to map other budgeted learning problems with large number of sensors to our DAG architecture and demonstrate empirical performance exceeding state-of-the-art algorithms for data composed of both few and many sensors.

C.1.a. Concept

We briefly present some of the mathematics that govern much of our approach. Note that in our context, the statistical models governing sensor measurements are unknown. Our network of classifiers/sensors setup is described in Figure 2 (on the next page) for the purpose of illustration. For explosives detection, one could acquire measurements first from a mm-wave scanner. Based on these measurements, one may decide whether or not to require a part/full-body inspection by a different technique. The main difference between the conventional decision scheme and our problem is that we also incorporate throughput in addition to detection accuracy. We will show in some of our experiments that we can obtain the same accuracy with 50% increase in throughput.

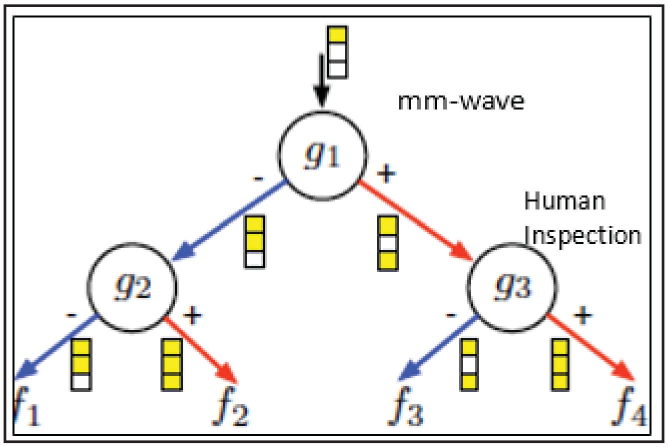


Figure 2: An example decision system of depth two: node g_1 (x_1) selects either to acquire sensor 2 for a cost c_2, or 3 for a cost c_3. Node $g_2(x_1, x_2)$ selects either to stop and classify with sensors {1, 2}, or to acquire 3 for c_3 and then stop. Node g_3 (x_1, x_3) selects to classify with {1, 3}, or with {1, 2, 3}.

C.1.b. Theory

A data instance, X, can consist of M sensor measurements, x = (x_1, x_2, ... x_M). Each data instance has a label (threat and type of threat, or not-a-threat) and in general belongs to one of the L classes indicated by its label y. Each sensor's throughput rate is encoded in terms of a cost measure, C_m. We represent our decision system as a binary tree. The binary tree is composed of K leafs and K - 1 internal nodes. At each internal node, j, is a binary decision function, sign (g_j(x)). This function determines which action should be taken for a given example. The binary decisions, g_j(x)'s, represent actions from the following set: stop and classify with the current set of measurements, or choose which sensor to acquire next. Each leaf node, k = 1, ... K, represents a terminal decision to stop and classify based on the available information. We assume that the classifiers (or detectors) at each leaf, f_k (x), are given and fixed. We propose methods for learning these detectors as part of our second thrust. Our objective here is to learn the decision functions: g_j (x)'s. The learning problem can be described in terms of a risk-minimization objective:

$$R(\mathbf{g},\mathbf{x},y)=\sum_{k=1}^{K}R_k(f_k,\mathbf{x},y)G_k(\mathbf{g},\mathbf{x})$$

Here g=(g_1, g_2, ... g_K) is the set of decision functions corresponding to the different imaging modalities (sensor measurements) and R_k(f_k,x,y) is the risk of making a decision at a leaf k . It consists of two terms: error of the classifier at the leaf, and the cost of sensors acquired along the path from the root node to the leaf. S_k is this set of sensors, and α is a parameter that controls trade-off between acquisition cost and classification error.

$$R_k(f_k,\mathbf{x},y)=\mathbb{1}_{f_k(\mathbf{x})\neq y}+\alpha\sum_{m\in S_k}c_m$$

Our goal is to find decision functions that minimize the average empirical risk, namely,

$$\min_{\mathbf{g}}\mathbb{E}_{\mathcal{D}}\left[R(\mathbf{g},\mathbf{x},y)\right]$$

Unfortunately, the objective is not only non-convex, but the decision at any stage, j, is hopelessly coupled (dependent) on decisions made at earlier stages as we see from the equation below:

$$\min_{\mathbf{g}} \sum_{i=1}^{N} R(\mathbf{g}, \mathbf{x}_i, y_i) =$$
$$\sum_{i=1}^{N} \sum_{k=1}^{K} \overbrace{R_k(f_k, \mathbf{x}_i, y_i)}^{\text{risk of leaf } k} \underbrace{\prod_{j=1}^{K-1} [\mathbb{1}_{g_j(\mathbf{x}_i)>0}]^{\mathbf{P}_{k,j}} [\mathbb{1}_{g_j(\mathbf{x}_i)\leq 0}]^{\mathbf{N}_{k,j}}}_{G_k(\cdot) = \text{ state of } \mathbf{x}_i \text{ in a tree}}$$

where, $P_{k,j}$ takes binary values and is one, if and only if, on the path to leaf k, a decision node j takes a positive decision. Similarly, N_{kj} also takes binary values and is one, if and only if, on the path to leaf k, a decision node j takes a negative decision.

For this reason, the state-of-the-art has considered special cases of this objective either by ignoring information from earlier stages and/or myopic settings (a scenario where only one sensor is going to follow next).

C.2. Results in Year 3: Adaptive Sensor Acquisition based on Directed Acyclic Graphs

In Year 3, we developed a new adaptive sensor acquisition system learned using labeled training examples. The system, modeled as a DAG, is composed of internal nodes, which contain decision functions, and a single sink node (the only node with no outgoing edges (see Fig. 3 on the next page)), representing the terminal action of stopping and classifying (SC). At each internal node, a decision function routes an example along one of the outgoing edges. Sending an example to another internal node represents acquisition of a previously un-acquired sensor, whereas sending an example to the sink node indicates that the example should be classified using the currently acquired set of sensors. The goal is to learn these decision functions such that the expected error of the system is minimized subject to an expected budget constraint.

First, we consider the case where the number of sensors available is small, though the dimensionality of data acquired by each sensor may be large (such as an image taken in different modalities). In this scenario, we construct a DAG that allows for sensors to be acquired in any order and classification to occur with any set of sensors. In this regime, we propose a novel algorithm to learn node decisions in the DAG by emulating dynamic programming (DP). In our approach, we decouple a complex sequential decision problem into a series of tractable cost-sensitive learning sub-problems. Cost-sensitive learning (CSL) generalizes multi-decision learning by allowing decision costs to be data dependent. Such reduction enables us to employ computationally efficient CSL algorithms for iteratively learning node functions in the DAG. In our theoretical analysis, we show that given a fixed DAG architecture, the policy risk learned by our algorithm converges to the Bayes risk as the size of the training set grows.

Next, we extend our formulation to the case where a large number of sensors exist, but the number of distinct sensor subsets that are necessary for classification is small (where the depth of the trees is fixed to 5). For this regime, we present an efficient subset selection algorithm based on sub-modular approximation. We treat each sensor subset as a new "sensor," construct a DAG over unions of these subsets, and apply our DP algorithm. Empirically, we show that our approach outperforms state-of-the-art methods in both small and large-scale settings.

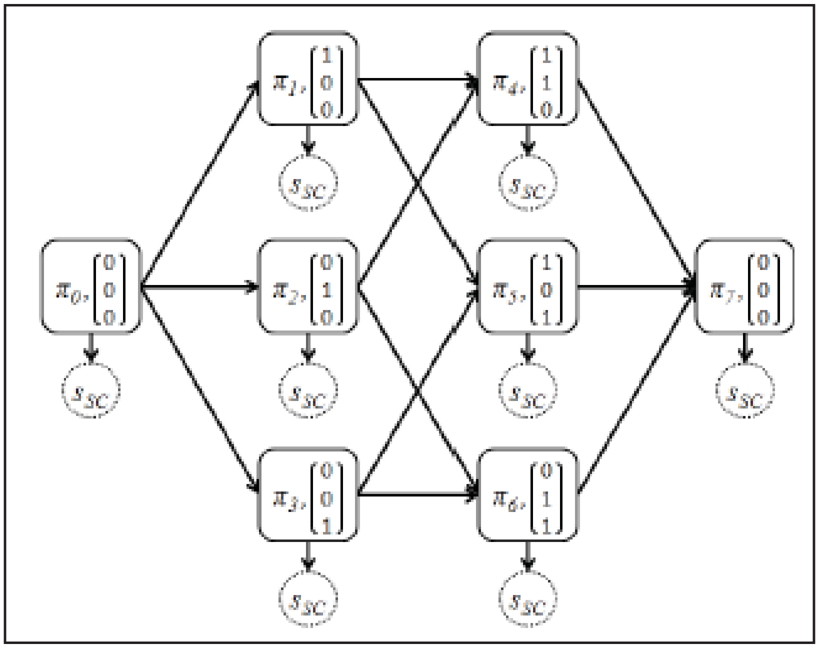


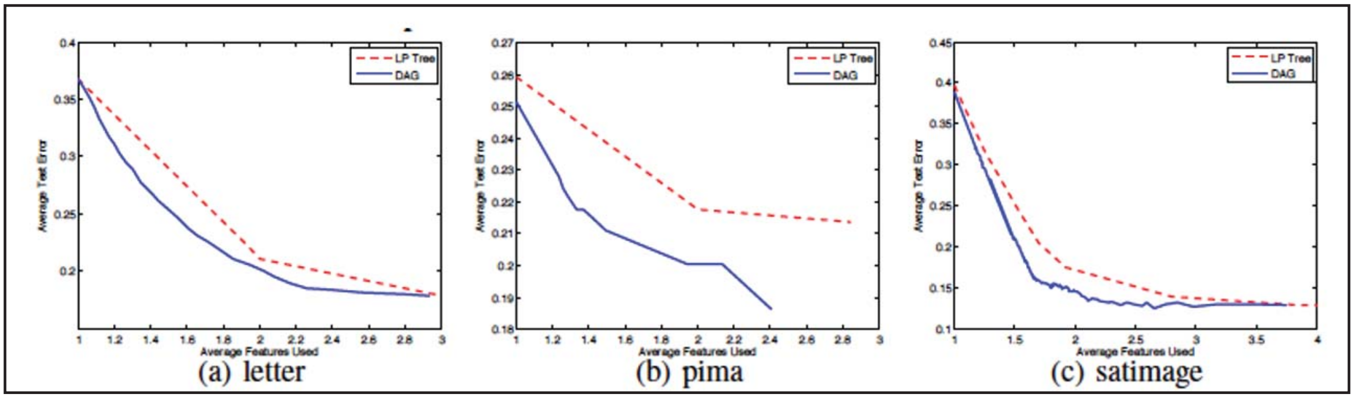
Figure 3: A simple example of a sensor selection DAG for a three sensor system. At each state, represented by a binary vector indicating measured sensors, a policy chooses between either adding a new sensor or stopping and classifying. Note that the state S_{sc} has been repeated for simplicity.

C.2.a. Experiments

We have compared our approach to existing state-of-the-art techniques, including myopic approaches, as well as alternative minimization techniques. The discriminative myopic strategy rejects observations by thresholding classification confidence at each stage. This strategy does not consider future costs, instead it looks only at current uncertainty and is therefore considered myopic. The non-convex (alternative minimization) algorithm attempts to minimize the empirical risk of the system using alternating minimization. After a random initialization, the algorithm attempts to optimize each decision function, g, by fixing all other decision functions and minimizing the empirical risk.

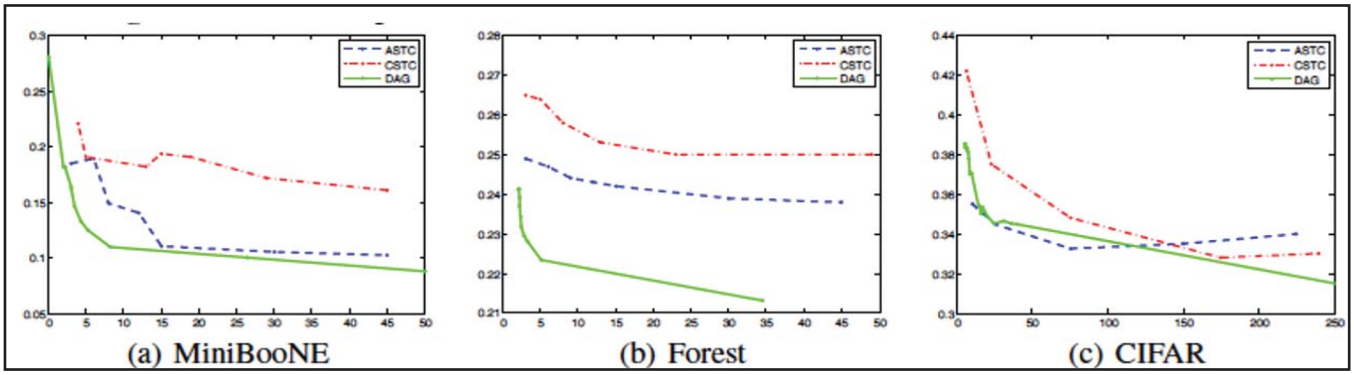
We performed experiments on several datasets including the threat dataset. Our results are based on the datasets chosen from UCI machine learning repository. As seen in Figure 4 (on the next page), our algorithm outperforms the conventional myopic strategy and achieves the same performance as the inefficient alternative minimization method. More importantly, these results also show that we can double the throughput while achieving nearly the optimal accuracy.

Unlike our LP tree work [13], which could only scale to small feature dimensions, our new DAG method can scale to very large data sets with large feature dimensions. We simulate performance of our method against benchmark datasets and compare it to several state-of-the-art algorithms below.



(a) letter (b) pima (c) satimage

Figure 4: Average number of sensors acquired vs. average test error comparison between LP tree systems and DAG systems.



(a) MiniBooNE (b) Forest (c) CIFAR

Figure 5: Comparison between CSTC, ASTC, and DAG of the average number of acquired features (x-axis) vs. test error (y-axis).

As seen in Figure 4, the systems learned with a DAG outperform the LP tree systems. Additionally, the performance of both of the systems is significantly better than previously reported performance on these data sets for budget cascades. This arises due to both the higher complexity of the classifiers and decision functions as well as the flexibility of sensor acquisition order in the DAG and LP tree compared to cascade structures. For this setting, it appears that the DAG approach is superior approach to LP trees for learning budgeted systems.

Figure 5 shows performance comparing the average cost vs. average error of CSTC, ASTC, and our DAG system. The systems learned with a DAG outperform both CSTC and ASTC on the MiniBooNE and Forest data sets, with comparable performance on CIFAR at low budgets and superior performance at higher budgets.

C.2.b. Results on Explosive Simulants Dataset

We now describe some of our results on a dataset containing explosive simulants, provided by Reveal Imaging. This dataset contains images taken of people wearing various simulants, obtained by different sensing modalities at a modest standoff distance. The imaging is done in three modalities: IR, PMMW, and AMMW. All the images are registered to a common coordinate system. We extract many patches from the images and use them as our training data. We learn threat/no threat detectors for this training data using an approach that will be described in Section C.3. For the purpose of describing our experiment here, a patch carries a binary label such that it either contains a threat, or it is clean. IR and PMMW are the fastest imaging modalities but also less informative. AMMW is slow since it requires raster scanning a person but it is the most useful. There are a total of 1,230 body images in the dataset.

We use this data set to illustrate our adaptive screening technique. The idea is to determine which types of imagery should be collected on each individual. An example of a basic inspection strategy is illustrated in Figure 6. Initially, a PMMW image may be examined for indicators of concealed objects. Subsequently, an IR image can also confirm the presence of such concealed objects. Finally, an AMMW image can be used to provide sufficiently discriminative information to classify the object as a threat. Note that, after each image is collected, the system can decide there is no threat present, thereby avoiding the extra effort to collect the additional imagery.

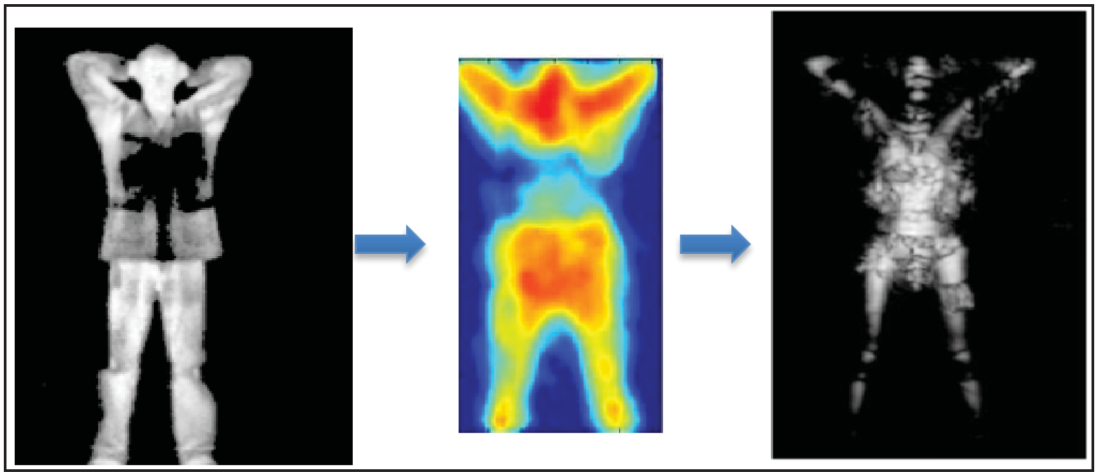


Figure 6: Illustration of Inspection Strategy consisting of three different scanning schemes.

We also obtained ROC curves that highlight the advantages of using our inspection strategy over a centralized approach, wherein the person is scanned with all the sensor modalities before any decision is made. Figure 7 (on the next page) illustrates the performance of the adaptive system with different sensing budgets, parameterized by the reject rate: the percentage of individuals that require AMMW information to determine a good threat/no threat decision. Note that at a 50% reject rate, we obtain the same detection/false alarm performance as a centralized system where all the sensor measurements are first obtained before any decision is made, indicating that our adaptive system would use AMMW in only 50% of the individuals in the system.

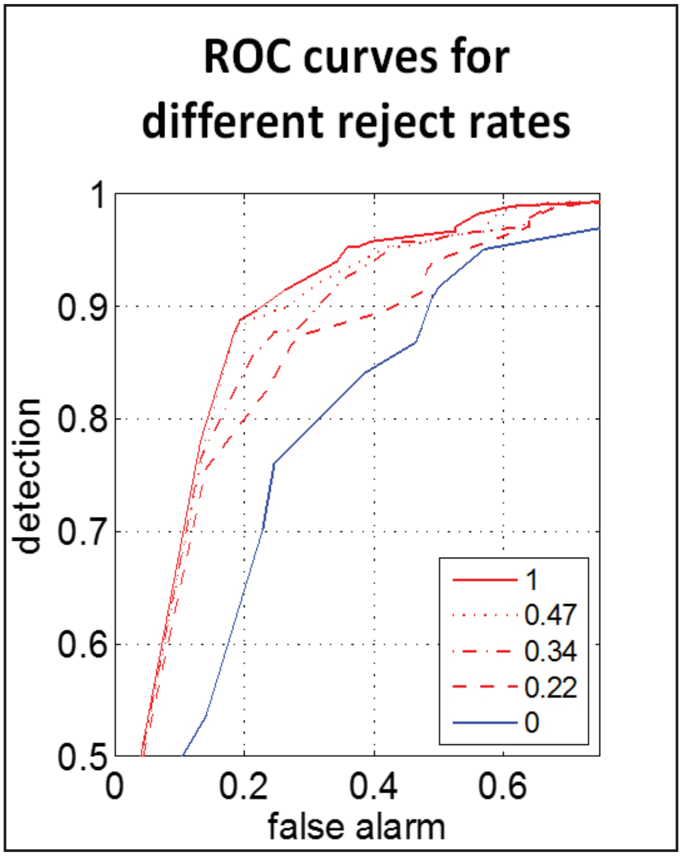


Figure 7: ROC curves for adaptive inspection scheme with different sensing budgets. The different curves correspond to the average number of instances when AMMW is utilized for detecting threats. Thus the blue curve is the baseline and corresponds to the case when AMMW is never used. We note that with 47% AMMW utilization, the ROC performance is close to using 100% AMMW utilization, i.e., on all subjects.

D. Major Contributions

We have developed new approaches for adaptive classifiers that can separate test cases into explosive threats, non-threats, and ambiguous objects needing further attention, in a Bayes optimal manner; taking into account the relative costs of different types of errors plus the cost of additional tests. These techniques have been applied successfully in many real-world datasets increasing the sensitivity and specificity of the automated decisions. The underlying assumption is that there is an expensive, but very accurate, mode of detection (e.g. manual inspection) that should be invoked infrequently.

Our recent work [4,14,15] is based on Prediction Time Cost Reduction approach [16]. Specifically, we assume a set of training examples in which measurements from all the sensors or sensing modalities, as well as the ground truth labels are available. Our goal is to derive sequential reject classifiers that reduce cost of measurement acquisition and error in the prediction (or testing) phase.

We developed a novel adaptive acquisition system based on DAG where internal nodes correspond to sensor subsets, and decision functions at each node choose whether to acquire a new sensor or classify using the available measurements. This problem can be posed as an empirical risk minimization over training data. Rather than jointly optimizing such a highly coupled and non-convex problem over all decision nodes, we propose an efficient algorithm motivated by dynamic programming. We learn node policies in the DAG by reducing the global objective to a series of cost sensitive learning problems. Our approach is computationally efficient and has proven guarantees of convergence to the optimal system for a fixed architecture.

E. *Milestones*

A significant milestone that was achieved was the development of data-driven approaches for designing multi-stage adaptive detection systems using different modalities, which optimizes detection performance when sensing throughput is constrained. This is applicable to the design of high-throughput screening algorithms for checkpoint as well as checked luggage environments. These algorithms were documented and published in highly competitive open literature publications (Wang et. al. NIPS 2015, Nan et. al. ICML 2015).

F. *Future Plans*

Since the project was not recommended for continued funding, there are no future plans.

III. RELEVANCE AND TRANSITION

A. *Relevance of Research to the DHS Enterprise*

- Development of multi-sensor ATR algorithms for check point and checked luggage that maintain throughput constraints.
- Development of adaptive sensing algorithms for risk-based screening at checkpoints
- Improved probability of false alarm and probability of detection while maintaining needs system throughput at checkpoints.

B. *Potential for Transition*

- Improved ATR concepts for AIT are of particular interest to mm-wave imaging and X-ray backscatter imaging vendors.
- Improved algorithms for exploitation of real time sensing information in adaptive risk-based screening for checkpoint and checked luggage applications.

C. *Transition Pathway*

We presented our results at workshops to industry practitioners, and will continue to discuss potential pathways for transition with our industrial partners.

D. *Customer Connections*

Due to the speculative, basic research nature of the work, we have not pursued customer connections at this time. The research is targeted for future system concepts.

IV. PROJECT ACCOMPLISHMENTS AND DOCUMENTATION

A. *Peer Reviewed Journal Articles*

1. M. Rohban, V. Saligrama, & D.M. Vaziri. "Minimax Optimal Sparse Signal Recovery with Poisson Statistics." IEEE Transactions on Signal Processing, 64(13), February 2016, pp. 3495 – 3508. DOI:10.1109/TSP.2016.2529588

B. *Peer Reviewed Conference Proceedings*

1. J. Wang, K. Trapeznikov, & V. Saligrama. "Efficient Learning by Directed Acyclic Graph For Resource

Constrained Prediction." 2015 Neural Information Processing Systems (NIPS), Montreal, Canada, December 7-12, 2015.

2. F. Nan, J. Wang, & V. Saligrama. "Feature-budgeted random forest." Proceedings of the 32nd International Conference on Machine Learning, JMLR: W&CP, Volume 37, Lille, France, July 6-11, 2015.

C. *Software Developed*

1. Algorithms:
    a. Group Membership Prediction, ICCV 2015
    b. Zero-Shot Learning via Semantic Similarity Embedding, ICCV 2015

V. REFERENCES

[1] Z. Xu, O.Chapelle, and K.Weinberger. The greedy miser: Learning under test-time budgets, In Proceedings of the 29th International Conference on Machine Learning, 2012.

[2] Z. Xu, M. Kusner, M. Chen, and K. Weinberger. Cost-sensitive tree of classifiers. In Proceedings of the 30th International Conference on Machine Learning, pages 133–141, 2013.

[3] Matt J. Kusner, Wenlin Chen, Quan Zhou, Zhixiang Eddie Xu, Kilian Q Weinberger, and Yixin Chen. Featurecost sensitive learning with submodular trees of classifiers. In Twenty-Eighth AAAI Conference on Artificial Intelligence, 2014.

[4] F. Nan, J. Wang, K. Trapeznikov, and V. Saligrama. Fast margin-based cost-sensitive classification. In International Conference on Acoustics, Speech and Signal Processing, 2014.

[5] V. S. Sheng and C. X. Ling. Feature value acquisition in testing: A sequential batch test algorithm. In Proceedings of the 23rd International Conference on Machine Learning, pages 809–816, 2006.

[6] Tianshi Gao and Daphne Koller. Active classification based on value of classifier. In Advances in Neural Information Processing Systems, volume 24, pages 1062–1070, 2011.

[7] Shihao Ji and Lawrence Carin. Cost-sensitive feature acquisition and classification. Pattern Recognition, 40(5):1474–1485, 2007.

[8] Sergey Karayev, Mario J Fritz, and Trevor Darrell. Dynamic feature selection for classification on a budget. In International Conference on Machine Learning: Workshop on Prediction with Sequential Models, 2013.

[9] G. Dulac-Arnold, L. Denoyer, P. Preux, and P. Gallinari. Datum-wise classification: a sequential approach to sparsity. In Machine Learning and Knowledge Discovery in Databases, pages 375–390. 2011.

[10] He He, Hal Daume III, and Jason Eisner. Imitation learning by coaching. In Advances in Neural Information Processing Systems, pages 3158–3166, 2012.

[11] R. Busa-Fekete, D. Benbouzid, and B. K´egl. Fast classification using sparse decision dags. In Proceedings of the 29th International Conference on Machine Learning, pages 951–958, 2012.

[12] K. Trapeznikov and V. Saligrama. Supervised sequential classification under budget constraints. In International Conference on Artificial Intelligence and Statistics, pages 581–589, 2013.

[13] Joseph Wang, Tolga Bolukbasi, Kirill Trapeznikov, and Venkatesh Saligrama. Model selection by linear programming. In European Conference on Computer Vision, pages 647–662, 2014.

[14] F. Nan, J. Wang, and V. Saligrama. Feature-budgeted random forest. In Proceedings of the 32nd International Conference on Machine Learning, 2015.

[15] J. Wang, K. Trapeznikov, V. Saligrama, Efficient Learning by Directed Acyclic Graph for Resource

Constrained Prediction, NIPS 2015.

[16] P. Kanani and P. Melville. Prediction-time active feature-value acquisition for cost-effective customer targeting. In Advances in Neural Information Processing Systems, 2008.