Use of Pattern Recognition in Detection of Improvised Explosive Devices

Jorge Buenfil, PhD candidate
US Army Armament Research, Development and Engineering Center (ARDEC)

20160427

Distribution A: Approved for Public Release: Distribution is unlimited.
Mobility/movement patterns and their implication in the CIED problem.
Mobility

• Let an AUS be a particular area under surveillance that contains no Improvised Explosive Devices (IEDs) at time zero \( t_0 \) and which might be penetrated by an agent carrying an IED at time \( t_k \). Then \( E = AUS_{t_0} \rightarrow AUS_{t_k} \) is an event of the form \( e \in \{null, IED\} \) which results in either no IED introduced in the AUS or an IED introduced in the AUS. The event \( e \) consists of a potential carrier (human, animal or machine) crossing the threshold of the AUS with or without an IED.

• Therefore, mobility patterns are of great importance for detection of IEDs.

• Regarding the aspect of mobility randomness, in the CIED domain mobility randomness is not desirable. Mechanisms and policies are usually set in place to prevent random mobility by groups or individuals to control their flow.
Mobility Patterns Considered

• Individual:
  1. Follow pathway (expected)
  2. Loiter
  3. Turn around
  4. Run\textsuperscript{[1]}

• Group:
  1. Clustering
  2. Occlusions

Methods of pattern recognition and their strengths, weaknesses, and constraints with respect to anomaly detection.
Anomaly vs. Pattern Recognition

–Anomaly Detection:
  • Statistical deviation from a norm
  • Looks for evidence of interruptions in energy flows
  • Computationally simple [2]
  • Usually direct observation

–Pattern Recognition:
  • Hypothesizes the class of objects perceived by the sensors by matching to learned models [3]
  • Feature vectors
  • Good for indirect observation

Pattern Recognition Methods

1. Statistical
   - Easy to compute
   - Well developed method

2. Syntactic
   - Easy to understand
   - Compact rules

3. Analysis by Synthesis
   - Exploit knowledge of the solution domain [4] [5]

4. Artificial Neural Networks
   - Formal Analysis
   - Availability of libraries [6]
   - Non-linear functions [7]

5. Perceptron
   - Ideal for DSPs
   - Multiple layers [8] [9]

Parameters to judge the "goodness" of the system
System Parameters

1. Adaptability
2. Manpower Reduction
3. Cost Reduction
4. Design for Robustness
5. Open architecture
Beyond quality and false negatives

Test says you don't have it

You really don't have it

TRUE NEGATIVE

You really do have it

FALSE POSITIVE

FALSE NEGATIVE

TRUE POSITIVE
Beyond Quality and False Negatives

- **Quality** and **low rate of false negatives** are variables of the system in operation, as opposed to the parameters of the system at architecture and design time.

- **High reliability** measured in terms of mean time between failures (\(MBTF\)) and mean time to repair (\(MTTR\)).

- **Plays well with others**: lack of interference with normal operations of this includes physical obstruction of normal operations of other systems (physical and electronic.)
System Optimization

System-Level Design

- Application model
  - Safety critical
  - Complex functionality
- System platform model
  - Heterogeneous/mixed
  - Incremental design

System-level design tasks

Model of system implementation

Analysis
  - Schedulability analysis
  - Communication delay analysis

Software synthesis
Hardware synthesis
Architectural Pillars

1. Modularity
2. Scalability
3. Simplicity
4. Openness
5. Common Standards
Capabilities and limitations of the techniques discussed
System Capabilities and Limitations

1. Adaptability
2. Manpower reduction
3. Cost Reduction
4. Design for Robustness
5. Open architecture
Layering the techniques to address the utility function
Layering of Techniques

The system architecture combines all those techniques into a coherent framework that meets the conditions necessary to support the utility function.

Using an open architecture, based on widely accepted standards, I propose to have a 3-layer approach.

1. **Framework**: The first layer is the basic framework architecture where elements that compute the results (threat assessment values for individuals, groups and the whole AoI) are identified and encapsulated; I call this part the Inference Engine (IE).

2. **Logical Architecture**: The second layer of the architecture is the logical model of the system. Logical because it exists in the realm of ideas and math, not in the physical sense of an actual system.

3. **Physical Architecture**: The third layer of the architecture is a physical instantiation of the second layer. At this level system functionality is allocated to software, hardware or a mix of them.
Gaming the system.
Anti-spoofing

- Attackers would not be able to use the adaptability of the system to their advantage is because the system is not fully automatic.
- the human-in-the-loop as a sensor is responsible for inspecting the AoI.
- The human operator in conjunction with security personnel on the ground coordinate random checks and questioning people and pat downs.
- the system dynamics portion of the Threat Assessment function would gradually elevate the sensitivity of the whole system by noticing via feedback loops an increase in suspicious readings, even when those readings do not cross the threshold of a system alert.
Measuring approach for quantifying the detection process.
System Metrics

- Let $A_x$ be a discrete assessment of threat made by an individual sensor $x$ in the range $[0.0, 1.0]$.
- Let $W_x$ be a weight assigned to sensor $x$ in the range $[0.0, 1.0]$.
- Each individual sensor reading is weighted by a factor that represents the relative confidence assigned to that individual sensor regarding its potential determination that an IED is present in the Aol.
- Let $TA_x$ denote the weighted Threat Assessment of sensor $x$ on a person $p$.
- Then for each person in the Aol their Threat Assessment Level $TAL_p$ which includes adjustment factors given by pattern analysis if applicable is given by:
  \[ TAL_p = \text{Max}(TAx_1, \ldots, TAx_n) \]
- The DFV at time $k$ is the highest Threat Assessment Level (TAL) of the Aol.
  \[ DFV = \max(TAL_{p_1}, \ldots, TAL_{p_n}) \]
- The DFV must satisfy the following two conditions:
  \[ DFV \geq 0 \text{ and } DFV \leq 1 \]
- The area-wide detection is quantified by a value, called Threat Assessment Value (TAV) which represents the probability of the presence of an IED in the Area of Interest (Aol).
- A value of 0.0 would represent absolute confidence that there is no IED in the Aol at the moment of the estimation. A value of 1.0 would represent absolute certainty that there is at least an IED in the Aol. The values in between correspond to different estimated probabilities that an IED is present given the detection of indicators of threat without being able to ascertain absolute certainty one way or another.
The DFV is modified by a feedback loop from a system dynamics engine that provides temporary effects on the current estimation based on prior estimations according to Bayes Rule. For example, if DFV at time $k-1$ was elevated beyond a set threshold that indicates what is the statistical DFV given current conditions of number of people in the AoI, time of day, weather conditions, Day of the week, etc. A positive factor is applied to the DFV at time $k$ to elevate the threat level accordingly. This is done because of the assumption that higher than usual DFVs, but still below the alert-level, could mean that multiple individuals with moderately elevated threat levels may collaborate and assemble an IED from parts each one carried into the AoI. The system dynamics model applies a decay rate to this factor of accumulated threat indication, in order to dissipate the extra indication of risk of threat and avoid a self-reinforcing loop that would produce a false alarm otherwise.

Finally, the TAV is the result of multiplying the DFV for the AoI by the systems dynamics model weight factor at time $t_k$.

- **Precision**
  - Relevant IED Detection ($tp/(tp + fp)$)

- **Recall**
  - Fraction of IEDs found ($tp/(tp + fn)$)

- Naïve Bayes Classifier
What exactly is the detection system measuring?
What the System Measures

- The system measures abnormal conditions with regards to normal scans of the human body under magnetic, infrared, microwave sensors, as well as behavioral deviations from the normal gait and biometric information.
- The detection system attempts to indirectly detect improvised explosive devices by applying pattern matching methods on the potential carriers of the IEDs.
Relationship of outcome metric with the ones collected from different internal approaches such as pattern identification, image processing, non visual inputs, etc.
Data Fusion

- Naïve Bayesian Classifier in conjunction with a dynamic system with reinforcing feedback loops.
Superiority of the multi-entry approach.
Multi-tiered/multi-entry approach

- To show true superiority of the multi-tiered/multi-entry approach the proposed system needs to demonstrate improvements over an existing non-tiered solution
- Not only in terms of quality of predictions of IED presence and low false negatives, but also in terms of Adaptability, Manpower reduction, Cost reduction, Design for Robustness, and Openness of the architecture
- The best approach is to use past data of another system the US Army has in place or has investigated with intent of development. This I would consider the ultimate test.
Validation plan
Validation Plan

The validation plan for this system is also a multi-tiered approach:

- The first level of validation is to validate the logic of the CIED system. For this I plan to analyze the algorithms and formulas mathematically.
- The second level of validation is to run the CIED application as a computer simulation, where instead of having actual sensors providing the data I will use Montecarlo techniques on probability density functions that approximate the sensing capabilities of the actual sensors planned to be used for the prototype system.
- The third level of validation is experimental. An actual prototype system is planned to include some of the most important sensor types. The software will run on Raspberry Pi microcomputers for signal preprocessing and the data fusion and inference engine will be hosted on a suitable computer that will act as the C2 system. The plan is to have a scaled down version of the actual system being proposed as proof of concept.
Validation Plan 2

- With regard to the availability of real data, yes it is correct that the data is classified.
- I have access to the data to use for comparisons.
- One possibility to handle the aspect of availability of the data to my academic committee is to "sanitize" the actual data.
- Alternatively, some members of my committee have the appropriate security clearance to look at the real data without any modifications and verify my findings.
System Design

C-IED Adaptive Network Implementation

- Dynamic system
- Data fusion
- Requirements Architecture Design Implementation Test Validation

- Day cameras
- IR cameras
- Thermal cameras
- CCTV
- Background detection
- Facial Recognition
- Image Processing
- Magnometer
- Non Visual Inputs
- Human expertise
- Adaptive Behavior
- Pattern Identification
- Pattern Analysis
- Pattern Recognition

- Display Monitor
- Countermeasures
- Human Validation
- Alarm Bells
- Traffic Control Actuators
- Prediction
- Adaptive Learning
- Bayesian Methods
- Kalman Filter
- Threat Assessment

Distribution A: Approved for Public Release: Distribution is unlimited.
Example table for each of the methods.
Innovative Armaments Solutions for Today and Tomorrow

Summary of Techniques

<table>
<thead>
<tr>
<th>Day Cameras</th>
<th>IR Cameras</th>
<th>Thermal sensors</th>
<th>Background Extraction</th>
<th>Facial Recognition</th>
<th>Gait Analysis</th>
<th>Magnetofermers</th>
<th>Human Expertise</th>
<th>Pattern Recognition</th>
<th>Adaptive Learning</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cameras by themselves do not possess adaptability, they always work the same.</td>
<td>The cameras by themselves do not possess adaptability, they always work the same.</td>
<td>The sensors by themselves do not possess adaptability, they always work the same.</td>
<td>Background Extraction is inherently adaptable because the algorithms do not use a static image of the area to use as background. Instead they do some image processing to determine which aspects of the scene are immovable and subtracts them from the scene to highlight the parts that are changing.</td>
<td>Facial Recognition, even though it can adjust for angles, lighting of the picture and some other minor changes, is not usually considered adaptable because it only recognizes faces that are actually contained in database. Cannot recognize someone new basing the recognition on fragmentation features from other people, for example.</td>
<td>Just like with Background Extraction, the system will go into degraded mode of operation if the Facial Recognition module fails.</td>
<td>The magnets by themselves are probably the least adaptable part of the system since this device does one and only one thing, detect metal in a specified amount or larger.</td>
<td>Definitely the most adaptable part of the system. Humans are capable of modifying their behavior according to circumstances even in the presence of new stimuli never seen before.</td>
<td>There is some degree of adaptability in Pattern Recognition modules based on statistical methods, which take into consideration evidence to compute a current prediction of which pattern is a best match for the new features discovered.</td>
<td>Adaptive learning is the mechanism by which the system gains its adaptability. Characteristics, other than using Human Expertise.</td>
</tr>
<tr>
<td>Human operators use the day cameras to observe suspicious behavior highlighted by the system and to direct countermeasures where appropriate. GOS cameras sometimes use these cameras to fuse this normal view with additional information on the operator screen.</td>
<td>IR cameras are used for low light and to see through haze and fog. The images are blended with visible light to enhance the context of images for human operators to read more rapidly.</td>
<td>Thermal sensors provide a way to indirectly detect explosive devices on some kind of an electronic signature from the heat emissions captured by the thermal sensors.</td>
<td>There are software routines running on the images from day cameras. Free open source libraries available.</td>
<td>The ability to identify people using facial recognition and matches them against a black list is a significant function for the system. The software that is tailored for the applications needed is available to use.</td>
<td>The system requires multiple IR cameras in order to cover the whole AoI. Should any of all IR Cameras become unavailable, the system would continue working but in degraded mode, informing the human operator of this condition.</td>
<td>The system architecture allows for use of practically any COTS or GOS cameras by providing a standard interface plus the ability to create customized interfaces using a framework.</td>
<td>The system requires a couple of Thermal sensors. Similarly to Background Extraction, the system will continue operations degraded mode and will notify the human operator.</td>
<td>Adaptive learning is the hardest subsymbol in terms of software. The reason for this is that its methodologies and behaviors are built into the core of the main system controller module. Replacing it would entail modifying the main system controller, swapping out the code already there. This is a no no in military, but also requires deep knowledge of the COTS SDL architecture, design, coding standards and dependencies of associated software elements.</td>
<td></td>
</tr>
<tr>
<td>Day cameras for CCTV are abundant in offerings and vary from $18 for a camera module for a Raspberry Pi 3 with an appropriate GOS; on to $40K for high end GigE cameras.</td>
<td>Anywhere from $252 for a basic camera for the Raspberry Pi computer to high-end $40K long range imaging cameras.</td>
<td>About $100 for a basic model to around $40K for military-grade equipment.</td>
<td>There are software routines available as open source libraries to process visual images such as Open Source Computer Vision Library (OpenCV), and the Dlib C++ Library.</td>
<td>Some as with Background Extraction and Facial Recognition, the system will continue working, but in degraded mode, if the Gait Analysis fails to work at some point.</td>
<td>The system architecture allows for use of practically any COTS or GOS magnetic sensors by providing a standard interface plus the ability to create customized interfaces using a framework.</td>
<td>Distribution A: Approved for Public Release: Distribution is unlimited.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| The system requires multiple day cameras in order to cover the whole AoI. Should any of all Day Cameras become unavailable, the system would continue working but in degraded mode, informing the human operator of this condition. | The system requires a couple of Thermal sensors. Similarly to Background Extraction, the system will continue operations degraded mode and will notify the human operator. | The system requires multiple IR cameras in order to cover the whole AoI. Should any of all IR Cameras become unavailable, the system would continue working but in degraded mode, informing the human operator of this condition. | The system architecture allows for use of practically any COTS or GOS cameras by providing a standard interface plus the ability to create customized interfaces using a framework. | The system architecture allows for use of practically any COTS or GOS thermal sensor by providing a standard interface plus the ability to create customized interfaces using a framework. | Another example of a service provide to the SDL that can be replaced as indicated in the case of Facial Recognition and Background Extraction. | The COTS SDL sees the human as a sensor. The human operator can also be replaced as long as the new operator is familiar with the way of interacting with the system (protocols) and meets the criteria for skills in the operation of the system, which is provided by training. | The CE2 SDL sees the human as a sensor. The human operator can also be replaced as long as the new operator is familiar with the way of interacting with the system (protocols) and meets the criteria for skills in the operation of the system, which is provided by training. | The COTS SDL sees the human as a sensor. The human operator can also be replaced as long as the new operator is familiar with the way of interacting with the system (protocols) and meets the criteria for skills in the operation of the system, which is provided by training.
• The final threat assessment is computed by applying a customized *Kalman filter* which estimates the *a posteriori* threat assessment as a linear combination of an *a priori* threat assessment and a weighted difference between a current threat assessment value and a threat assessment prediction on the next threat assessment value.

\[
\hat{x}_k = \hat{x}_k^- + K(z_k - H\hat{x}_k^-)
\]

• \(\hat{x}_k\) is the *a posteriori* threat assessment.
• \(\hat{x}_k^-\) is the *a priori* threat assessment.
• \((z_k - H\hat{x}_k^-)\) is the residual, the discrepancy between the predicted threat value \(H\hat{x}_k^-\) and the current threat value \(z_k\).
• \(K\) is an \(n \times m\) matrix that represents the gain or blending factor that minimizes the *a posteriori* error covariance.