Pattern Recognition Inference Engine for Improvised Explosive Device Detection

Presented to:
4th Annual SERC Doctoral Students Forum
16 December 2016
Methods of pattern recognition, their strengths, weaknesses, and constraints with respect to anomaly detection.
—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


What exactly is the detection system measuring?
• 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.
1. Adaptability
2. Manpower Reduction
3. Cost Reduction
4. Design for Robustness
5. Open architecture
1. Modularity
2. Scalability
3. Simplicity
4. Openness
5. Common Standards
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 \( k \) \( (t_k) \). Then is an event of the form which results in either no IED introduced in the AUS or an IED introduced in the AUS. The event 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.
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.)
Layering the techniques to address the utility function
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, the C-IED system is built with 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.
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 AoI.

Let $TA_x$ denote the weighted Threat Assessment of sensor $x$ on a person $p$.

Then for each person in the AoI their Threat Assessment Level $TAL_p$ which includes adjustment factors given by pattern analysis if applicable is given by:

$$TAL_p = Max(TA_{x_1}, ..., TA_{x_n})$$

The DFV, Data Fusion Value, at time $k$ is the highest Threat Assessment Level (TAL) of the AoI.

$$DFV = Max(TAL_{p_1}, ..., TAL_{p_n})$$

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 (AoI).

A value of 0.0 would represent absolute confidence that there is no IED in the AoI at the moment of the estimation. A value of 1.0 would represent absolute certainty that there is at least an IED in the AoI. 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 $t_{k-1}$ 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 $t_k$ 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 system 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
SYSTEMEMIGRAM OF METRICS

Distribution A: Approved for Public Release: Distribution is unlimited.
• Naïve Bayesian Classifier in conjunction with a dynamic system with reinforcing feedback loops.
GAMING THE SYSTEM

Distribution A: Approved for Public Release: Distribution is unlimited.
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.
Distribution A: Approved for Public Release: Distribution is unlimited.
To show 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 similar system in operation in order to contrast and compare results. Initial conversations have started to explore the feasibility of such approach with the US Army.