Aneet Kumar Dutta
Computer Science & Engineering Department
IIT Kanpur
10/05/2019

Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructures, IIT Kanpur.

Introduction

- This presentation is on Intrusion Detection System based on the paper "Truth Will Out:Departure-Based Process Level Detection of Stealthy Attacks on Control Systems" by Wissam Aoudi,Mikel Iturbe and Magnus Almgren.
- PASAD: Novel attack detection mechanism by monitoring time series data.
- Structural changes in process behavior can be detected.

Concept

- The mathematical representation of the normal behavior is obtained.
- The training vectors(belongs to normal behavior) are projected onto a signal subspace and the centroid of that cluster is obtained.
- The test vectors are then projected onto the signal subspace and euclidean distance is calculated between the projected test vectors in the subspace and the centroid obtained from the projected training vectors.
- A threshold is set, if the projected test vector is at greater distance than the threshold then that point is treated as an attack

Four Steps of PASAD

- Step 1: Embedding
- Step 2: Singular value Decomposition
- Projection onto the Signal Subspace
- Distance Tracking

Embedding

- Let $x_1, x_2, x_3, \ldots\ldots\ldots x_N$ be an uni-variate real valued time series, L be a lag parameter or the window size and $K = N - L + 1$.
- Trajectory matrix is derived from the time series data which is a Hankel matrix.
- $$X = \begin{bmatrix} x_1 & x_2 & x_3 & \ldots\ldots\ldots & x_k \\ x_2 & x_3 & x_4 & \ldots\ldots\ldots & x_{k+1} \\ x_3 & x_4 & x_5 & \ldots\ldots\ldots & x_{k+2} \\ . & . & . & \ldots\ldots\ldots & . \\ . & . & . & \ldots\ldots\ldots & . \\ . & . & . & \ldots\ldots\ldots & . \\ x_L & x_{L+1} & x_{L+2} & \ldots\ldots\ldots & x_N \end{bmatrix}$$
- The columns are the lagged vectors.

Singular Value Decomposition

- Deterministic behavior of the control system is determined by obtaining the eigen vectors of the lag-co-variance matrix XX^T
- SVD(X)=$U\Sigma V^T$
  The columns of U and the columns of V are called the left-singular vectors and right-singular vectors of X respectively.
  The left-singular vectors of X are a set of orthonormal eigenvectors of XX^T.
- Therefore, eigen vectors are obtained from the column vectors of U and r leading eigen vectors are chosen where r is the degree of deterministic variability.
  $U = u_1, u_2, ...u_r$, a $L * r$ matrix

Projection onto Signal Subspace

- Let L^r be the subspace spanned by the column vectors of U.
- The centroid of the cluster formed in L^r is $\tilde{c} = Pc$ where c is the sample mean of the lagged vectors and P is the Projection matrix
- $P = UU^T$, but here using Isometric trick $P = U^T$
- Using Isometric trick helped to reduce computational cost and complexity.

Distance Tracking

- Each test vector x_j is projected onto the signal subspace L^r by $U^T x_j$
- Departure score is calculated which is the Euclidean distance between the projected test vector and the centroid of the cluster.
  $D_j = ||\tilde{c} - U^T x_j||^2$
- If $D_j > \theta$(threshold) then an alert is generated for the test vector.

Threshold Determination

- $\theta = max\{D_{n,r,\tau} : N < n < \tau\}$ where $D_{n,r,\tau}$ is the departure score corresponding to observed in specified range.
- In Tenesse Eastman Dataset,first 500 observation is used for training.
  Then, D_j is measured for next 3500 observations and the maximum value of D_j is set as threshold. Attack is started from 4000^{th} observation.
- In SWaT Dataset,first 4000 observation is used for training.
  Then, D_j is measured for next 3000 observations and the maximum value of D_j is set as threshold.

Tenesse Eastman:Attack1

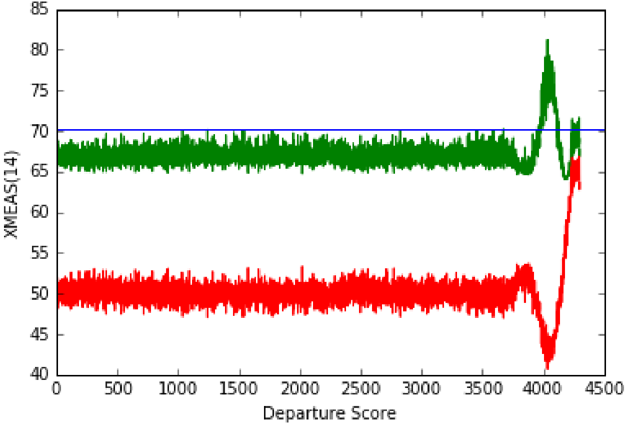

Figure: The red line represents the sensor reading with time.The green represents the Departure score.The blue line represents the threshold.When the sensor measurements deviates from its normal behavior there is a peak in the departure score which depicts anomaly is detected

Tenesse Eastman:Attack2

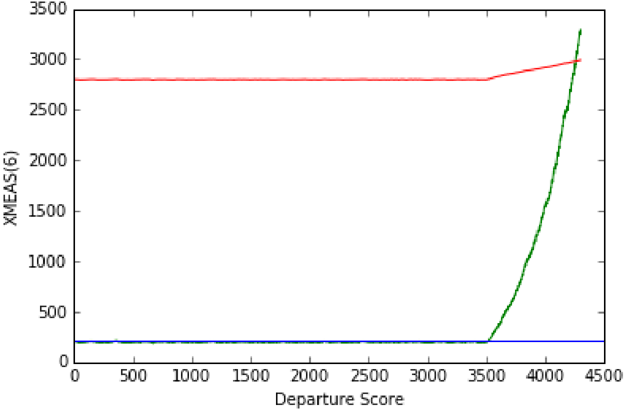

Figure: The red line represents the sensor reading with time.The green represents the Departure score.The blue line represents the threshold.When the sensor measurements deviates from its normal behavior there is a peak in the departure score which depicts anomaly is detected

SWaT:Attack1

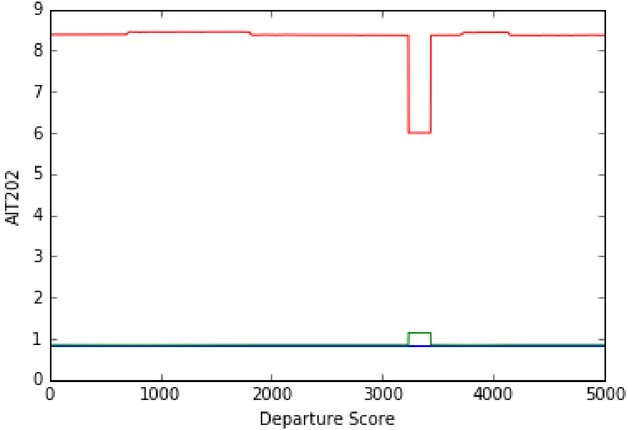

Figure: The red line represents the sensor reading with time.The green represents the Departure score.The blue line represents the threshold.When the sensor measurements deviates from its normal behavior there is a peak in the departure score which depicts anomaly is detected

SWaT:Attack2

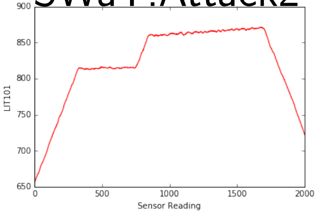

Figure: The red line represents the sensor reading with time.The tank is overflown at value > 800

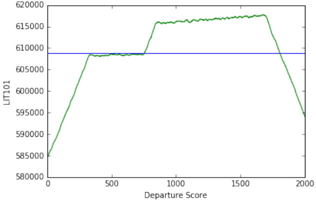

Figure: When the sensor reading > 800 the departure score is above the threshold value

Conclusion

- PASAD is able to detect attacks in both Tenesse Eastman dataset and SWaT dataset.
- Applying Isometric trick reduced computational cost which will help us to detect attacks in real time.
- The mathematical representation is derived for each variable/sensor separately. Thus we need to run this detection mechanism in parallel for each variable separately.