Cybersecurity Assignment 1

Mayank Sharma, 160392

August, 12, 2019

1

1.1

Since, the means of communication between the sensor is a computer network, an attacker having access to the network can send fake/corrupted readings (by impersonating **water level sensor**) to the PLC based controller (assuming that there isn't any kind of message authenctication protocol between the sensors and PLC Controller).

In this scenario, attacker will send readings that the water level is below the threshold, which in turn will prompt PLC Controller to open the valves, thereby causing a water overflow.

1.2

Similar to the above case, if the there isn't any kind of message integrity check between the **temperature sensor** and PLC Controller, an attacker can send readings which show low temperature to PLC Controller. The controller will try to increase the temperature (above any normal temperature), which may be catastrophic.

1.3

Some of the preventative measures we can employ in such a plant:

- The network must be secured from any outsider access or even for insiders, there must be different access privileges as to who can access the network directly. All the accesses to such a critical network should be monitored in real-time.
- The message integrity between the sensors and the controllers must be maintained by using something like HMAC.
- If possible, multiple sensors should be used and their individual readings should be looked at by the controllers. (Redundancy)
- An anomaly detection system may as well be deployed to detect any abnormal activity in the system.

2

From the defintion of inner product, we have

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T \mathbf{y}$$

So, for $\langle \mathbf{A}\mathbf{x}, \mathbf{y} \rangle$

$$\begin{aligned} \implies \langle \mathbf{A}\mathbf{x}, \mathbf{y} \rangle &= (\mathbf{A}\mathbf{x})^T \mathbf{y} \\ &= (\mathbf{x}^T \mathbf{A}^T) \mathbf{y} \\ &= \mathbf{x}^T (\mathbf{A}^T \mathbf{y}) \\ &= \langle \mathbf{x}, \mathbf{A}^T \mathbf{y} \rangle \end{aligned}$$

Hence, Proved.

3

Firstly, $det(\mathbf{A}) \neq 0$. Hence, the matrix $\mathbf{A}$ is invertible and we can proceed forward with its eigen-decomposition. For eigen values, we do $det(\mathbf{A} - \lambda\mathbf{I}) = 0$.

$$\begin{aligned} det(\mathbf{A} - \lambda\mathbf{I}) &= 0 \\ -x^3 + 14x^2 + 24x + 3 &= 0 \end{aligned}$$

The roots of the above equation are

$$\begin{aligned} \lambda_1 &= 15.5553 \\ \lambda_2 &= -1.41941 \\ \lambda_3 &= -0.13587 \end{aligned}$$

The corresponding eigenvectors (after normalization) are

$$\mathbf{v}_1 = \begin{bmatrix} 0.29983 \\ 0.68205 \\ 1 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} -0.963758 \\ -0.334138 \\ 1 \end{bmatrix}, \mathbf{v}_3 = \begin{bmatrix} 1.57302 \\ -2.39338 \\ 1 \end{bmatrix}$$

Now, the matrix $\mathbf{A}$ can be written as $\mathbf{A} = \mathbf{PDP}^{-1}$ where $\mathbf{P}$ is a square matrix whose i^{th} column is the i^{th} eigen vector of matrix $\mathbf{A}$ and $\mathbf{D}$ is the diagonal matrix with its diagonal elements as the eigenvalues of $\mathbf{A}$.

$$\begin{aligned} \mathbf{P} &= \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 \end{bmatrix} \\ \mathbf{D} &= diag(\begin{bmatrix} \lambda_1, & \lambda_2, & \lambda_3 \end{bmatrix}) \end{aligned}$$

So, we get

$$\begin{aligned} \mathbf{P} &= \begin{bmatrix} 0.29983 & -0.963758 & 1.57302 \\ 0.682059 & -0.334138 & -2.39338 \\ 1 & 1 & 1 \end{bmatrix} \\ \mathbf{P}^{-1} &= \begin{bmatrix} 0.397545 & 0.489735 & 0.546776 \\ -0.593726 & -0.245794 & 0.345663 \\ 0.196181 & -0.243941 & 0.107561 \end{bmatrix} \\ \mathbf{D} &= \begin{bmatrix} 15.5553 & 0 & 0 \\ 0 & -1.41941 & 0 \\ 0 & 0 & -0.135874 \end{bmatrix} \end{aligned}$$

To verify, we multiply the three matrices again, and we get

$$\mathbf{PDP}^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 4.99999 & 5.99999 \\ 7.00002 & 8 & 8.00001 \end{bmatrix} \approx \mathbf{A}$$

4

We know that the L-2 Norm of a vector $\mathbf{x}$ is given by,

$$\|\mathbf{x}_2\|_2^2 = \mathbf{x}^T\mathbf{x}$$

Since, $\mathbf{Q}$ is an orthogonal matrix, we have

$$\mathbf{Q}^T\mathbf{Q} = \mathbf{I} = \mathbf{Q}\mathbf{Q}^T$$

Now, left multiplying $\mathbf{x}$ with $\mathbf{Q}$ and gives us $\mathbf{Qx}$ which is an $n \times 1$ vector. Then taking its L-2 Norm, we get

$$\begin{aligned}
\|\mathbf{Qx}\|_2^2 &= (\mathbf{Qx})^T(\mathbf{Qx}) \\
&= \mathbf{x}^T\mathbf{Q}^T\mathbf{Qx} \\
&= \mathbf{x}^T\mathbf{Ix} \\
&= \mathbf{x}^T\mathbf{x} \\
&= \|\mathbf{x}\|_2^2
\end{aligned}$$

Hence, Proved.

5

Given that $\mathbf{S}$ is a symmetric matrix (i.e. $\mathbf{S} = \mathbf{S}^T$) with its eigenvectors $(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n)$ and the corresponding eigen values $(\lambda_1, \lambda_2, ..., \lambda_n)$. Now, by the property of symmetric matrices, these eigenvectors are orthogonal.

To Prove:

$$\mathbf{S} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \mathbf{v}_i^T$$

Now, we know that we can decompose $\mathbf{S}$ as $\mathbf{S} = \mathbf{PDP}^{-1}$, where $\mathbf{P}$ is a matrix whose columns are the eigenvectors of $\mathbf{S}$ and $\mathbf{D}$ is a diagonal matrix whose diagonal values are eigenvalues of $\mathbf{S}$.

$$\mathbf{P} = \left[\begin{array}{ccc} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 \end{array} \right]$$
$$\mathbf{D} = diag(\ \lambda_1, \ \ \lambda_2, \ \ \lambda_3 \ )$$

Since, $\mathbf{P}$ is an orthogonal matrix because all its column vectors are orthogonal, so we have $\mathbf{P}^{-1} = \mathbf{P}^T$.

$$\mathbf{S} = \mathbf{PDP}^{-1} = \mathbf{PDP}^T$$

$$\implies \mathbf{S} = \left[\begin{array}{cccc} \mathbf{v}_1, & \mathbf{v}_2, & \ldots, & \mathbf{v}_n \end{array} \right] \left[\begin{array}{cccc} \lambda_1, & 0, & \ldots, & 0 \\ \ldots, & \lambda_2, & \ldots, & 0 \\ \ldots, & \ldots, & \ldots, & \ldots \\ 0, & 0, & \ldots, & \lambda_n \end{array} \right] \left[\begin{array}{c} \mathbf{v}_1^T \\ \mathbf{v}_2^T \\ \ldots \\ \mathbf{v}_n^T \end{array} \right]$$

Once we multiply the above three matrices, we get

$$\mathbf{S} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \mathbf{v}_i^T$$

Hence Proved.

6

Given $\mathbf{A}_{m\times n}$ matrix, the kernel of $\mathbf{A}$ is defined as

$$\ker(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = 0\}$$

and the row space of $\mathbf{A}$ is defined as taking $\mathbf{A} = \begin{bmatrix} \mathbf{a}_1^T \\ \mathbf{a}_2^T \\ \dots \\ \dots \\ \mathbf{a}_m^T \end{bmatrix}$

$$\text{row}(\mathbf{A}) = \{\mathbf{y} \mid \mathbf{y} = \sum_{i=1}^{m} \mathbf{a}_i c_i, \qquad c_i \in \mathbb{R}\}$$

Now, from the defintion of ker $(\mathbf{A})$, we have

$$\begin{gathered} \mathbf{A}_{m\times n}\ \ \mathbf{x}_{n\times 1} = 0 \\ \implies \mathbf{a}_i^T\mathbf{x} = 0 \end{gathered}$$

To check for orthogonality, we arbitrarily take any vector $\mathbf{y}$ from row$(\mathbf{A})$ and similarly, $\mathbf{x}$ from ker$(\mathbf{A})$ and check using their inner product. If the inner product is 0, then the two spaces are orthogonal to each other.

$$\begin{aligned} \langle \mathbf{y}, \mathbf{x} \rangle &= \mathbf{y}^T\mathbf{x} \\ &= \left(\sum_{i=1}^{m} c_i\mathbf{a}_i\right)^T \mathbf{x} \\ &= \left(\sum_{i=1}^{m} c_i\mathbf{a}_i\right)^T \mathbf{x} \\ &= \left(\sum_{i=1}^{m} c_i\mathbf{a}_i^T\right) \mathbf{x} \\ &= \sum_{i=1}^{m} c_i(\mathbf{a}_i^T\mathbf{x}) \\ &= 0 \end{aligned}$$

Hence, the kernel space of $\mathbf{A}$ and row space are orthogonal to each other.

7

The SVD is defined as follows:
Let $\mathbf{A}$ be an $(m \times n)$ matrix with $m \geq n$. Then there exist orthogonal matrices $\mathbf{U}_{m\times m}$ and $\mathbf{V}_{n\times n}$ and a diagonal matrix $\Sigma_{(m\times n)} = \text{diag}(\sigma_1, \ldots, \sigma_n)$ with $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_n \geq 0$, such that

$$\mathbf{A} = \mathbf{U}\Sigma\mathbf{V}^T$$

The values σ_i are called the singular values of $\mathbf{A}$.

We know, If $\mathbf{A} = \mathbf{U}\Sigma\mathbf{V}^T$, then the column vectors of $\mathbf{V}$ are the eigenvectors of the matrix $\mathbf{A}^T\mathbf{A}$ and the column vectors of matrix $\mathbf{U}$ are the eigenvectors of the matrix $\mathbf{A}\mathbf{A}^T$.

Now, the matrices $\mathbf{A}^T\mathbf{A}$ and $\mathbf{A}\mathbf{A}^T$ are symmetrical (because $(\mathbf{A}^T\mathbf{A})^T = \mathbf{A}^T\mathbf{A}$, and $(\mathbf{A}\mathbf{A}^T)^T = \mathbf{A}\mathbf{A}^T$).

$$\mathbf{A}^T\mathbf{A} = (\mathbf{U}\Sigma\mathbf{V})^T(\mathbf{U}\Sigma\mathbf{V}) = \mathbf{V}\mathbf{D}\mathbf{V}^T,$$
$$\text{where } \mathbf{D} = \Sigma^T\Sigma = diag\ (\sigma_1^2, \ldots, \sigma_n^2)$$

Also,

$$\mathbf{A}\mathbf{A}^T = (\mathbf{U}\Sigma\mathbf{V})(\mathbf{U}\Sigma\mathbf{V})^T = \mathbf{U}^T\Sigma\Sigma^T\mathbf{U}^T,$$
$$\text{where } \Sigma\Sigma^T = diag\ (\sigma_1^2, \ldots, \sigma_n^2, 0, \ldots, 0)$$

We further re-instate the fact that $\mathbf{U}$ and $\mathbf{V}$ are orthogonal by the property that the eigenvectors of a symmetrical matrices (here, $\mathbf{A}^T\mathbf{A}$ and $\mathbf{A}\mathbf{A}^T$) are orthogonal.

Now, Calculating the SVD consists of finding the eigenvalues and eigenvectors of $\mathbf{A}^T\mathbf{A}$ and $\mathbf{A}\mathbf{A}^T$. The eigenvectors of $\mathbf{A}^T\mathbf{A}$ make up the columns of $\mathbf{V}$, and the eigenvectors of $\mathbf{A}\mathbf{A}^T$ make up the columns of $\mathbf{U}$.

Suppose the eigenvalues of $\mathbf{A}^T\mathbf{A}$ are $(\sigma_1, \ldots, \sigma_n)$ such that $(\sigma_1 \geq \sigma_2 \ldots \geq \sigma_n \geq 0)$ and corresponding eigenvectors are $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$, hence the singular values in Σ are $(\sqrt{\sigma_1}, \ldots, \sqrt{\sigma_n})$. Let $\lambda_i = \sqrt{\sigma_i}$, so that λ_i is a singular value of Σ. Also, let $\mathbf{u}_i = \frac{\mathbf{A}\mathbf{x}_i}{\lambda_i}$. The matrix $\mathbf{U}$ has the colums $\mathbf{u}_i$ and the matrix $\mathbf{V}$ has the colums $\mathbf{x}_i$.

Lets take a look at the multiplication in $\mathbf{A} = \mathbf{U}\Sigma\mathbf{V}^T$ step by step. Firstly, we have $\mathbf{U}$ which we multiply by the diagonal matrix $\Sigma_{m\times n}$ (with diagonal values set to σ_i, and possibly padded with zeros if we run out of eigenvalues). Hence, we get a matrix with colums (this is basically scaling the colums of $\mathbf{U}$ with factors equal to singular values in Σ)

Then, we multiple $\mathbf{U}\Sigma$ with $\mathbf{V}^T$, and the product contains terms like $\mathbf{A}\mathbf{x}_i\mathbf{x}_j^T$, but since $\mathbf{x}_i$ and $\mathbf{x}_j$ are the eigenvectors of a symmetric matrix, $\mathbf{x}_i$ and $\mathbf{x}_j$ form an orthogonal basis. The significance of multiplcation of V^T term is that it basically transforms (rotates) a matrix in the n-dimensional space.

Applications of SVD: SVD is used for dimensionality reduction, meaning that we can remove those components of a matrix which have very small singular values. This has the benefit that it reduces computation costs. This is highly used in lossy image compression in the cases where we're fine if we lose some information at the benefit of being able to store the image at a smaller size.