AEROSPANZA

TEAM: POWERPUFFF

PROBLEM STATEMENT: What cybersecurity challenges do air traffic control systems face, and what strategies can be implemented to protect air traffic control (ATC) infrastructure and ensure the safety and reliability of air traffic management?

ANOMALY DETECTION

Contents

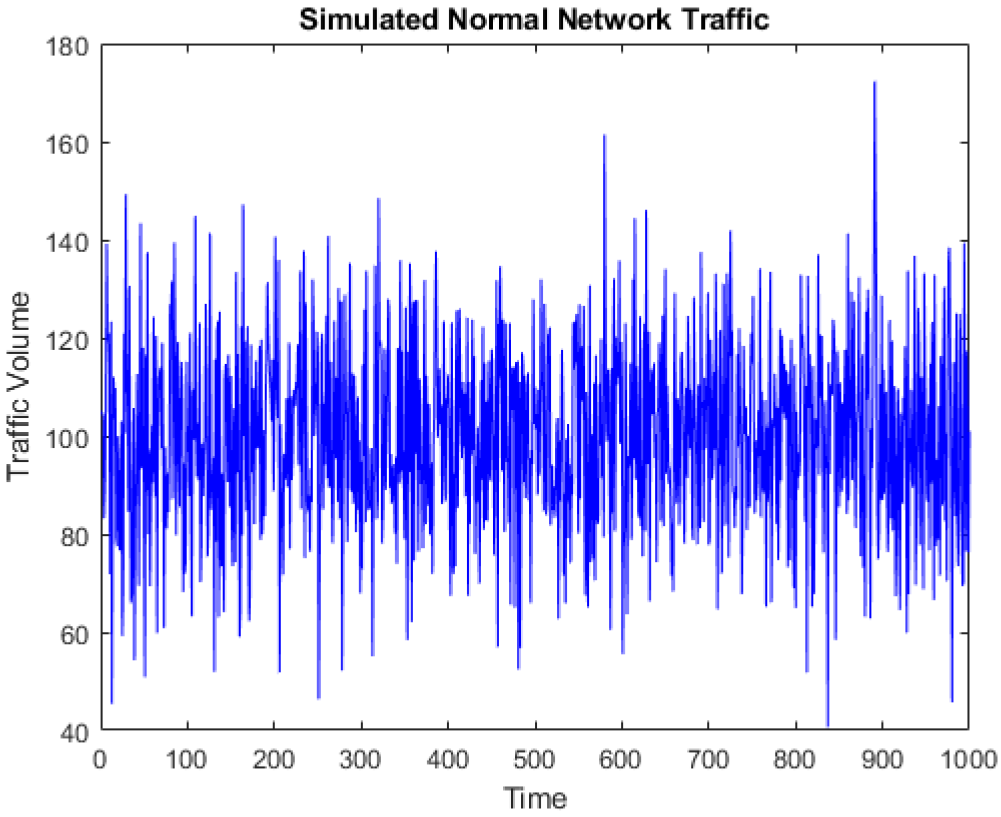
- Simulate Normal Network Traffic
- Introduce Anomalous Traffic (e.g., a spike)
- Dynamic Threshold Using Moving Average
- Anomaly Detection (Using Dynamic Threshold)
- Log and Trigger Alerts for Detected Anomalies

Code

```
% Clear all previous data

clc;

clear;
```

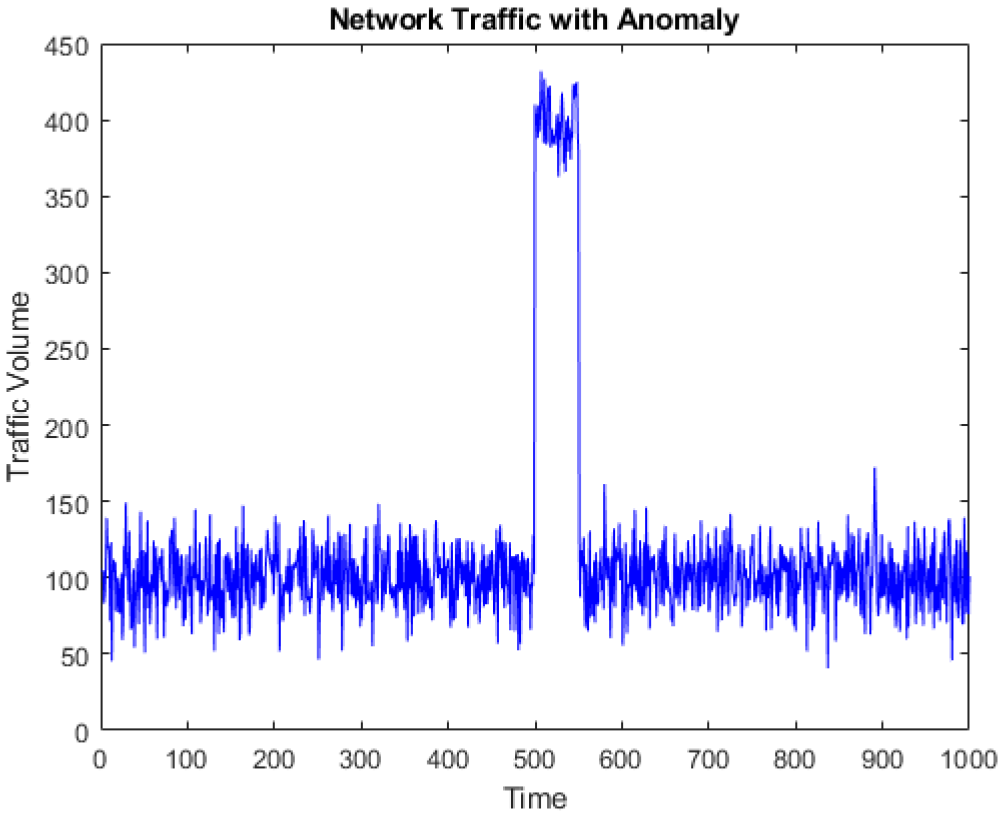
Step 1: Simulate Normal Network Traffic

```
n_time_steps = 1000;  % Total number of time steps

normal_traffic = 100 + 20*randn(1, n_time_steps);  % Normal traffic with randomness

% Plot the normal traffic

figure;

plot(normal_traffic, 'b');

title('Simulated Normal Network Traffic');

xlabel('Time');

ylabel('Traffic Volume');
```



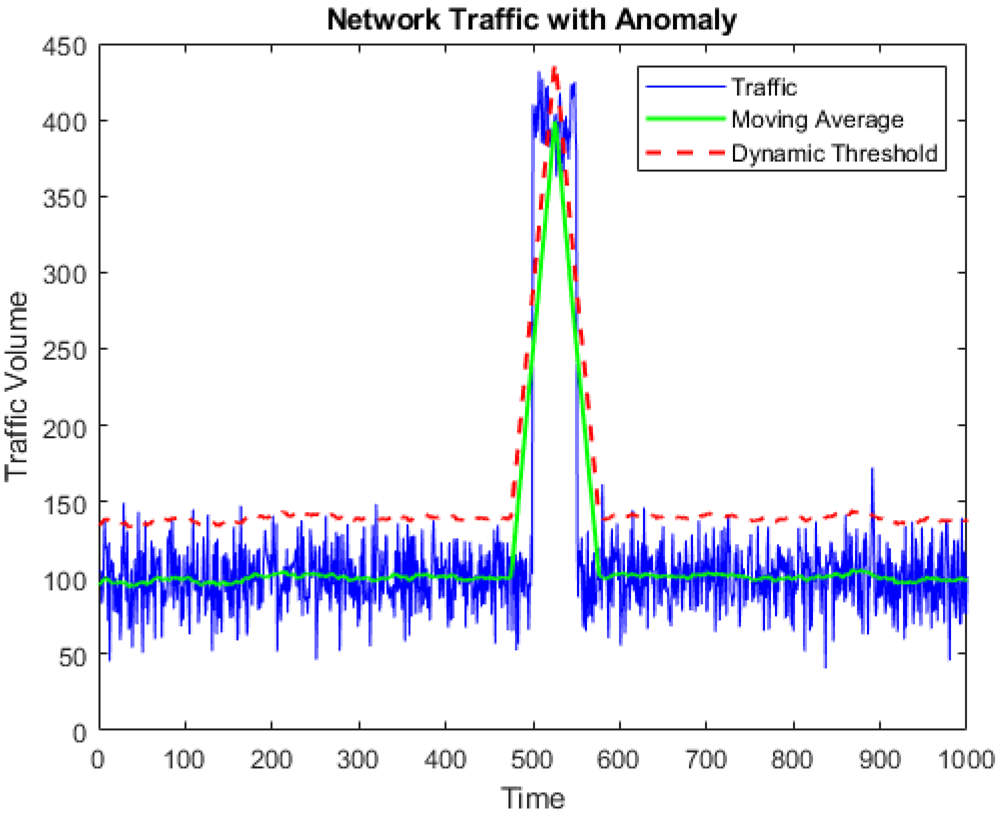
Step 2: Introduce Anomalous Traffic (e.g., a spike)

```
anomaly_start = 500;  % Start of anomaly

anomaly_duration = 50;  % Duration of the anomaly

anomaly_intensity = 300;  % How big the anomaly spike is


% Inject the anomaly

anomalous_traffic = normal_traffic;

anomalous_traffic(anomaly_start:anomaly_start + anomaly_duration) = ...

   anomalous_traffic(anomaly_start:anomaly_start + anomaly_duration) + anomaly_intensity;


% Plot the traffic with the anomaly

figure;

plot(anomalous_traffic, 'b');

hold on;

title('Network Traffic with Anomaly');

xlabel('Time');

ylabel('Traffic Volume');
```



Step 3: Dynamic Threshold Using Moving Average

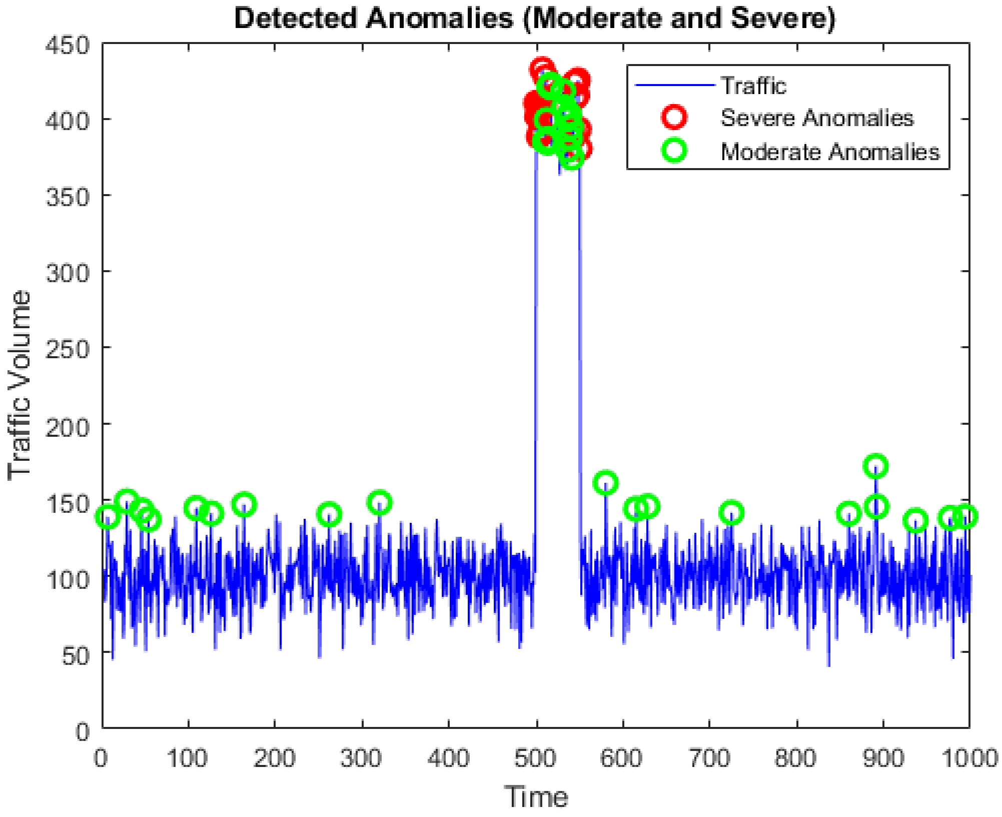
```
window_size = 50;  % Window size for the moving average

moving_avg = movmean(anomalous_traffic, window_size);  % Calculate moving average

dynamic_threshold = moving_avg + 2*std(normal_traffic);  % Dynamic threshold based on traffic fluctuations


% Plot the moving average and threshold

plot(moving_avg, 'g', 'LineWidth', 1.5);

plot(dynamic_threshold, 'r--', 'LineWidth', 1.5);

legend('Traffic', 'Moving Average', 'Dynamic Threshold');

hold off;
```



Step 4: Anomaly Detection (Using Dynamic Threshold)

```
detected_anomalies = anomalous_traffic > dynamic_threshold;  % Detect where traffic exceeds the dynamic threshold


% Log detected anomalies

anomaly_indices = find(detected_anomalies);

anomaly_values = anomalous_traffic(detected_anomalies);


% Display detected anomalies with severity classification

severe_anomalies = anomaly_values > dynamic_threshold(anomaly_indices) + 50;  % Severe anomalies

moderate_anomalies = ~severe_anomalies;  % Less severe anomalies


% Plot detected anomalies (severe and moderate)

figure;

plot(anomalous_traffic, 'b');

hold on;
```

```
plot(anomaly_indices(severe_anomalies), anomaly_values(severe_anomalies), 'ro', 'MarkerSize', 8, 'LineWidth', 2);  % Severe anomalies (red)

plot(anomaly_indices(moderate_anomalies), anomaly_values(moderate_anomalies), 'go', 'MarkerSize', 8, 'LineWidth', 2);  % Moderate anomalies (green)

title('Detected Anomalies (Moderate and Severe)');

xlabel('Time');

ylabel('Traffic Volume');

legend('Traffic', 'Severe Anomalies', 'Moderate Anomalies');

hold off;
```



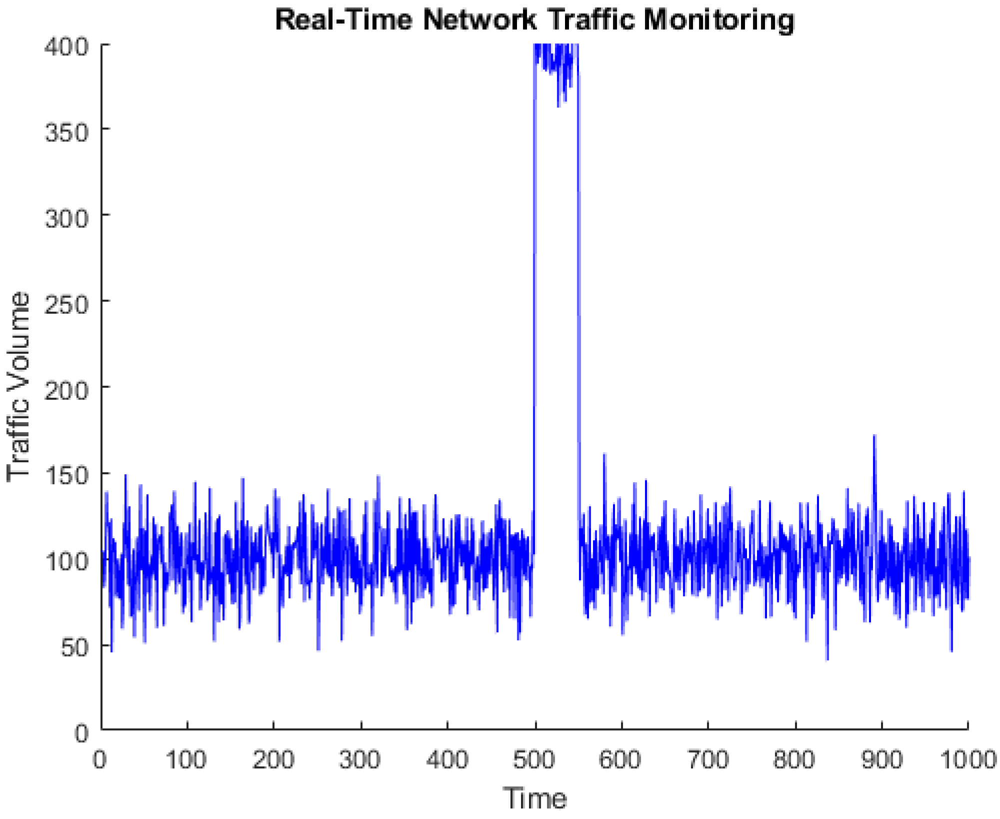
Step 5: Log and Trigger Alerts for Detected Anomalies

```
if any(detected_anomalies)

  disp('Alert: Anomalies detected in the network traffic!');

  disp('Logging anomalies:');

  for i = 1:length(anomaly_indices)

    if severe_anomalies(i)

      fprintf('Severe Anomaly at Time %d: Traffic = %.2f\n', anomaly_indices(i), anomaly_values(i));

    else
```

```
      fprintf('Moderate Anomaly at Time %d: Traffic = %.2f\n', anomaly_indices(i), anomaly_values(i));
    end
  end
else
  disp('No anomalies detected.');
end

% Simulate flight data and radar data alongside network traffic
flight_data = 50 + 10*randn(1, n_time_steps); % Simulate flight data (e.g., altitude or speed)
radar_data = 200 + 30*randn(1, n_time_steps); % Simulate radar data (e.g., plane positions)

% Apply anomaly detection for each system
flight_anomalies = flight_data > mean(flight_data) + 2*std(flight_data);
radar_anomalies = radar_data > mean(radar_data) + 2*std(radar_data);

% Combine and log anomalies from all systems
if any(flight_anomalies)
  disp('Anomalies detected in flight data!');
end
if any(radar_anomalies)
  disp('Anomalies detected in radar data!');
end

% Example real-time plot for monitoring network traffic
figure;
h = animatedline('Color', 'b');
axis([0 n_time_steps 0 400]);
xlabel('Time');
ylabel('Traffic Volume');
title('Real-Time Network Traffic Monitoring');
```

```
for t = 1:n_time_steps
    addpoints(h, t, anomalous_traffic(t)); % Real-time update of traffic data
    drawnow;
end

% Open a file to log anomalies
fileID = fopen('anomaly_log.txt', 'w');
fprintf(fileID, 'Time, Anomaly Type, Value\n');

% Log each anomaly with its type and time
for i = 1:length(anomaly_indices)
    if severe_anomalies(i)
        fprintf(fileID, '%d, Severe, %.2f\n', anomaly_indices(i), anomaly_values(i));
    else
        fprintf(fileID, '%d, Moderate, %.2f\n', anomaly_indices(i), anomaly_values(i));
    end
end
fclose(fileID);
```

```
Alert: Anomalies detected in the network traffic!
Logging anomalies:
Moderate Anomaly at Time 7: Traffic = 139.16
Moderate Anomaly at Time 29: Traffic = 149.29
Moderate Anomaly at Time 46: Traffic = 143.34
Moderate Anomaly at Time 54: Traffic = 137.47
Moderate Anomaly at Time 109: Traffic = 144.83
Moderate Anomaly at Time 126: Traffic = 141.39
Moderate Anomaly at Time 164: Traffic = 147.21
Moderate Anomaly at Time 262: Traffic = 140.79
Moderate Anomaly at Time 320: Traffic = 148.48
Severe Anomaly at Time 500: Traffic = 409.98
Severe Anomaly at Time 501: Traffic = 401.41
Severe Anomaly at Time 502: Traffic = 404.50
Severe Anomaly at Time 503: Traffic = 387.99
Severe Anomaly at Time 504: Traffic = 409.50
Severe Anomaly at Time 505: Traffic = 392.01
Severe Anomaly at Time 506: Traffic = 406.47
Severe Anomaly at Time 507: Traffic = 431.95
Severe Anomaly at Time 508: Traffic = 411.64
Severe Anomaly at Time 509: Traffic = 408.71
Moderate Anomaly at Time 510: Traffic = 384.73
Severe Anomaly at Time 511: Traffic = 426.93
Moderate Anomaly at Time 512: Traffic = 398.77
Moderate Anomaly at Time 513: Traffic = 383.90
Moderate Anomaly at Time 514: Traffic = 386.42
Moderate Anomaly at Time 515: Traffic = 420.68
Moderate Anomaly at Time 516: Traffic = 420.24
Moderate Anomaly at Time 517: Traffic = 422.13
Moderate Anomaly at Time 531: Traffic = 417.62
Moderate Anomaly at Time 532: Traffic = 407.28
Moderate Anomaly at Time 536: Traffic = 399.42
Moderate Anomaly at Time 537: Traffic = 379.26
Moderate Anomaly at Time 538: Traffic = 402.43
Moderate Anomaly at Time 539: Traffic = 386.85
Moderate Anomaly at Time 540: Traffic = 394.18
Moderate Anomaly at Time 541: Traffic = 374.15
Severe Anomaly at Time 542: Traffic = 392.17
Severe Anomaly at Time 543: Traffic = 388.05
Severe Anomaly at Time 544: Traffic = 423.15
Severe Anomaly at Time 545: Traffic = 413.54
Severe Anomaly at Time 546: Traffic = 423.36
Severe Anomaly at Time 547: Traffic = 414.99
Severe Anomaly at Time 548: Traffic = 424.89

Severe Anomaly at Time 549: Traffic = 392.71

Severe Anomaly at Time 550: Traffic = 380.15

Moderate Anomaly at Time 580: Traffic = 161.40

Moderate Anomaly at Time 615: Traffic = 144.40

Moderate Anomaly at Time 628: Traffic = 146.06

Moderate Anomaly at Time 725: Traffic = 141.90

Moderate Anomaly at Time 860: Traffic = 141.27

Moderate Anomaly at Time 891: Traffic = 172.36

Moderate Anomaly at Time 892: Traffic = 145.81

Moderate Anomaly at Time 937: Traffic = 136.72

Moderate Anomaly at Time 977: Traffic = 138.40

Moderate Anomaly at Time 994: Traffic = 139.31

Anomalies detected in flight data!

Anomalies detected in radar data!
```


Real-Time Network Traffic Monitoring
Traffic Volume
Time