Anomaly Detection in Industrial Networks

PSE GRUPPE

KOMPETENZZENTRUM FÜR ANGEWANDTE SICHERHEITSTECHNOLOGIE
Advisor: M.Sc. Ankush Meshram

This Document outlines the requirements (both functional and non-functional), environment, target audience, and use cases of the software described below.

Contents

1 Purpose **1**

2 Overall Description **1**

3 Interfaces **1**

4 Functional Requirements **1**

5 Data Requirements **1**

6 Non-Functional Requirements **1**

7 Essential Testcases **1**

8 Software Modelling **1**

8.0.1 GUI 1

8.1 Scenario 2

8.2 Use cases 2

8.2.1 Interactivity 2

8.3 Object Modelling 2

8.4 Dynamic Modelling 2

8.5 User Interface 2

8.6 Glossary 2

1 Purpose

The goal of this project is to create a software visualization tool for industrial network traffic to simplify the analysis of anomalous behaviour, both in realtime and from captured stored data.
This software is part of the ADIN framework and is refererred to as the "ADIN Inspector". One component to achieve this goal is a web interface built with modularity in mind so as to make it easily extendable.
The Web view is able to display a series of diagrams and charts to easily identify the behaviour of the network. Within the Web view the user has the ability to zoom, select, highlight, and filter out data to better understand the aforementioned behaviour in different OSI layers, as well as visualize the flow rate between network nodes.
To support this Web view a back-end messaging solution is needed. This allows the user to easily switch between multiple streams of captured data.

2 Overall Description

3 Interfaces

4 Functional Requirements

5 Data Requirements

6 Non-Functional Requirements

7 Essential Testcases

8 Software Modelling

8.0.1 GUI

The basic data structure needed for graphs are a given set of nodes and a given set of edges, as they are often drawn as node-link diagrams. In the postal data set, nodes could represent the origins and destinations of postal flows. Edges represent the flows between the respective origins and destinations.In intelligence analysis, investigators use semantic graphs to organise concepts and relationships as graph nodes and links in hopes of discovering key trends, patterns, and insights."

A key issue in graph visualisation is the size of the graph, i.e. the size of the data to visualise. With a growing amount of data to display, graphs can become too complex and overburdening for the analyst's cognitive capacity. It thus becomes difficult for the user to conduct significant analysis. Because of the issues described above, research often

focuses on ways to solve the problems of visual clutter, e.g. by aggregation or clustering techniques, which is also one of the main topics of cartographic generalisation.

8.1 Scenario

8.2 Use cases

8.2.1 Interactivity

Visual analytics methods combine interactive visualisations with automated analysis techniques. This allows the user to decide e.g. which part of the data he or she wants to explore in more detail.

A basic principle for visual data exploration was introduced by Shneiderman (1997) by what he called the "The Visual Information Seeking Mantra:

Overview first, zoom and filter, then details-ondemand". This lets the data analyst define to a certain level what he or she wants to see and visualise.

Similar to this, Bertin (1983) specified three "levels of reading,": The elementary level (allowing the analyst to look at the information about a single data record), the intermediate level (showing summarised information about a group of data records), and the global level (providing an overview of all data elements).

8.3 Object Modelling

8.4 Dynamic Modelling

8.5 User Interface

8.6 Glossary

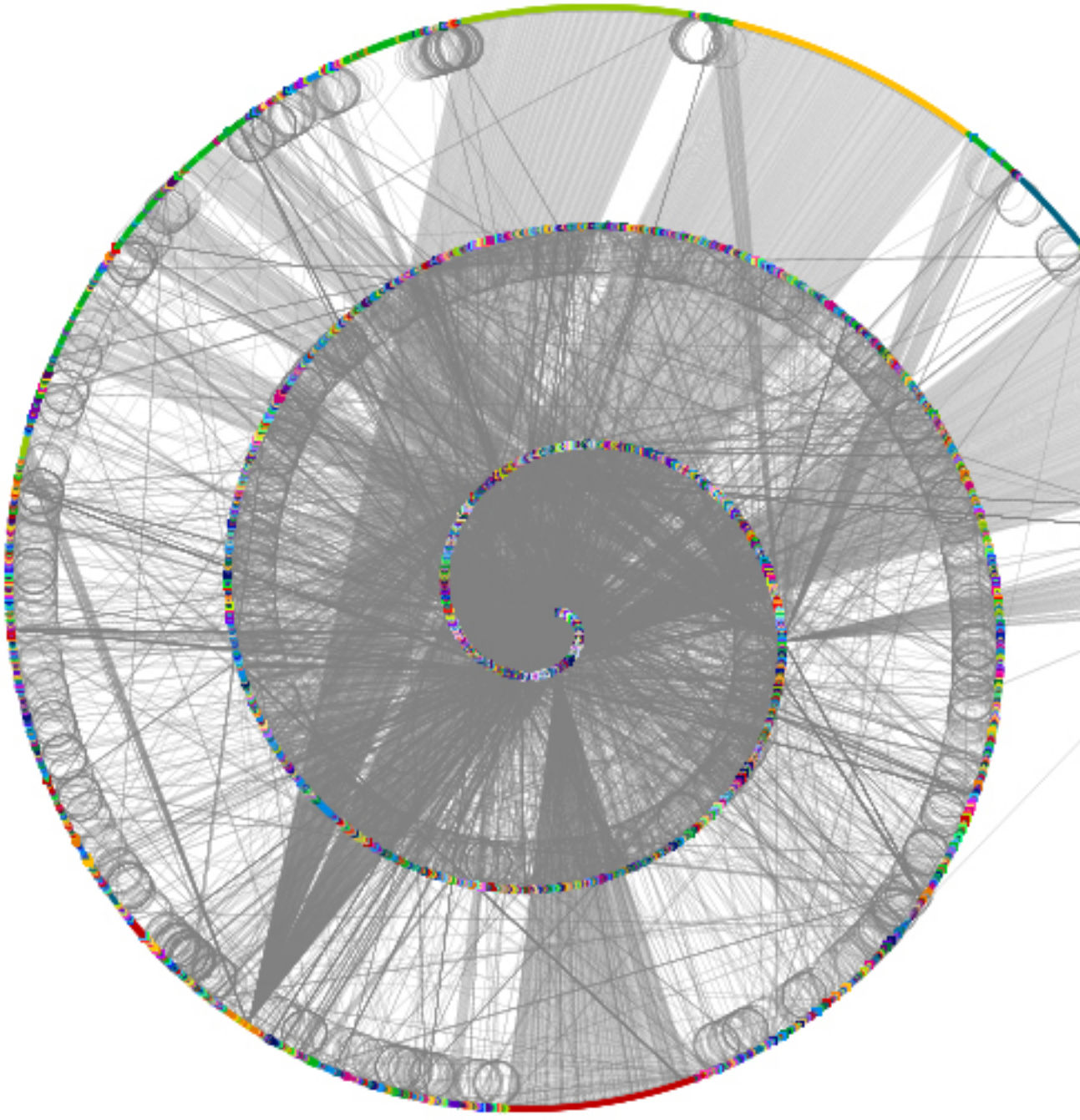

Figure 1: Node-Link-Graph