Dynamite: **Dyna**mic **M**onitoring **I**nterface for **T**ask **E**nsembles

Wolfgang Jentner, Mennatallah El-Assady, Dominik Sacha, Dominik Jäckle, and Florian Stoffel

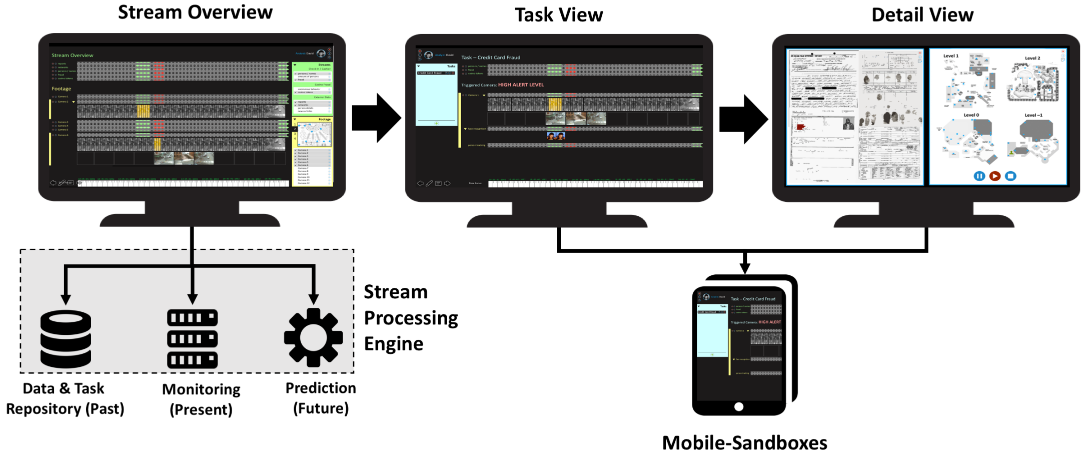


Fig. 1. The architecture of dynamite contains three levels of detail: a stream overview, a task view, and a detail view. Each is connected to the stream processing engine consisting of a data repository, monitoring, and a prediction facility. Mobile sandboxes containing data or views of the task- and detail views enable an effective communication with other personnel.

Abstract—Dynamite adopts a multi-level task-driven approach to support event surveillance and time critical decision making for large premises, e.g. casinos or holiday resorts. The system integrates with a complex stream processing engine processing various heterogeneous streams using task-based aggregates. These task stream ensembles are processed in three temporal dimensions to support investigators in examining or responding to threats: (1) automatically highlighting current stream anomalies (present - monitoring), (2) taking previously captured data streams and analysis sessions into account to provide the investigator with information and stream recommendations (past - information gathering support) and (3) predicting relevant upcoming events and scenarios (future - decision support). The system provides three interactive views: a stream overview, a task view, and a detail view that allow a team of investigators to collaborate on their monitoring and investigation tasks.

Index Terms—Decision Support, Overview-and-Detail, Stream Processing and Visualization

1 Introduction

A challenging task for security operators is to gain insight into ongoing events while keeping the overview and to not potentially miss any new upcoming events during the current investigation. Dynamite is a system designed to support investigators in such tasks. Thereby, its main purpose is to use the system collaboratively but it is also possible to work with it as a single user. Different visualizations each varying in detail allow the investigator to never lose track of the overview.

A use case that is used throughout this work describes a suspect using two different credit cards which are denied. In a third attempt and by using another card, the suspect is able to buy the desired chips used in the casino. However, dynamite is capable of handling a vast array of tasks due to the adaptive task-driven aggregation.

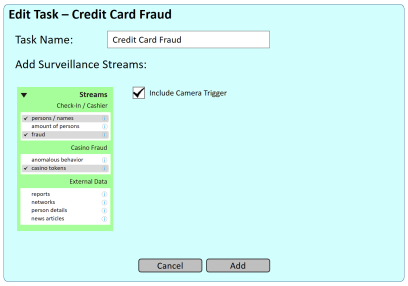
The architecture is described in the next Section. The following Section details about the different visualizations also introducing the novel HexaFlow streaming visualization technique. Section 4 describes the collaborative aspects of Dynamite. The work is concluded in Section 5 and future extensions and improvements are outlined.

2 Task-Driven Monitoring Architecture

Dynamite's architecture is shown in Figure 1. It is motivated by the following main ideas: (1) Task driven aggregation and combination of data streams, and (2) three level of details, that are defined by each task individually. Having a potentially large number of data streams available, the biggest issue is to make sense out of all the available information. A natural way to tackle this problem is to aggregate the streams [1]. Thus, reducing the amount of information to an almost arbitrary low level. For different tasks, such as VIP routing or fraud detection and investigation, different kinds of data and aggregation levels are necessary. Dynamite presents the investigator with three coordinated views enabling the investigator to drill down into the stream aggregates revealing more detailed information while preserving context to higher level aggregates. This supports the investigator in monitoring the current situation, selecting task dependent stream ensemble information and to request details on demand. Task definitions are stored in the task repository and can be maintained manually. Figure 2 shows a task creation wizard for managing task definitions such as "Credit Card Fraud Detection". The stream processing engine automatically analyzes the entire stream repository to identify correlating streams based on inter-dependent anomalies and complements the task definition with further (unbiased) information. The analyst workspace is divided to provide three different scopes: a high-level stream overview, a task view, and a detailed view.

- *All authors are with the University of Konstanz, Germany. Data Analysis and Visualization Group E-mail: forename.lastname@uni-konstanz.de*

Manuscript received xx xxx. 201x; accepted xx xxx. 201x. Date of Publication xx xxx. 201x; date of current version xx xxx. 201x. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org. Digital Object Identifier: xx.xxxx/TVCG.201x.xxxxxxx



Edit Task – Credit Card Fraud

Task Name: Credit Card Fraud

Add Surveillance Streams:

Streams

Check-In / Cashier
- ✓ persons / names
- amount of persons
- ✓ fraud

Casino Fraud
- anomalous behavior
- ✓ casino tokens

External Data
- reports
- networks
- person details
- news articles

☑ Include Camera Trigger

Fig. 2. The task creation wizard allows analysts to manage tasks by adding and removing streams from task definitions.

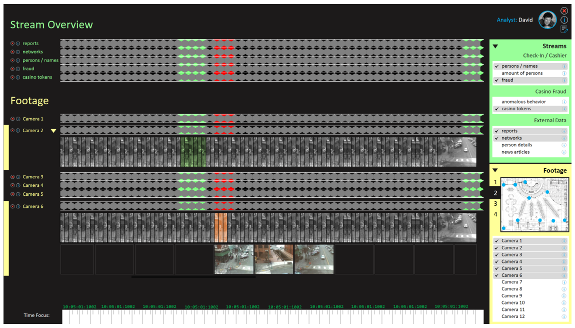


Fig. 3. Stream overview using HexaFlow visualizations.

3 Stream Visualization

3.1 Stream Overview

The stream overview provides insights into the current situation by showing a highly aggregated view of the available data streams with connections to current events on premises. To visualize data streams, we utilize a novel visualization technique called HexaFlow (Figure 3) that follows the ideas of Zhu and Shasha [2]. HexaFlow visualizations are based on temporal windows of the underlying data stream, which are visually depicted by hexagons. Each time window is plotted next to the previous time window keeping the stream metaphor intact. The triangle shaped free space between neighboring hexagons is used to indicate alert levels referring to the directly adjacent hexagons.

According to the alertness levels ”warning” and ”serious”, the triangles will be filled with a yellow and red color, respectively, if the stream does not contain any alerting data, the triangle will have no fill, e.g. be black in our examples. To make use of the space of the hexagons, their inner space can be utilized by the data streams in case of alerts. For video streams, stills from the video stream can be shown in the hexagon, dangerous weather conditions could be indicated by corresponding iconic displays.

3.2 Task View

This view (Figure 4) visualizes task dependent streams in more detail once a task has been selected or created. Task definitions can be chosen within the Stream Overview or in the taskbar on the left-hand side of the Task View. This lets the investigator efficiently switch between parallel tasks. Streams can be investigated in more detail by reordering, expand/fold operations, and time frame/event selections. Different stream detail visualizations are shown within the hexagons or underneath the selected streams/time frames. Note, that the temporal consistent alignment allows identifying stream dependencies and potential root causes For example in Figure 4, we can see that the person tracking stream starts revealing critical events when the face recognition identified a suspect in camera 1. Subsequently, more detailed information about the suspect and the person tracking is shown in the Detail View.

3.3 Detail View

The detail view adapts to the current task. For example, for tasks that built upon the information where a person is located on premises, the detail view may contain a floor plan and indication of the current or past positions of the person in question. Tasks that depend on news reports, or weather information, can be supported by a detail view giving access to the latest information from the news stream or weather forecasts. This makes the detail view an important, versatile and task-adaptive tool to give context or details to ongoing investigations. Additionally, the detail view can also serve as a reporting tool for the analyst.

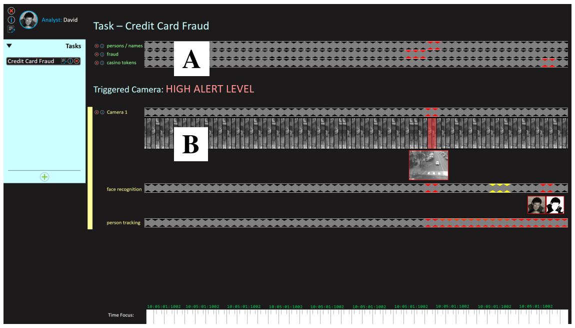


Fig. 4. Credit card fraud investigation task view. This view shows a condensed form of the streams generated by person/name detection, fraud detection, as well as the stream of the casino tokens *A* using the HexaFlow visualization technique. The corresponding camera details, triggered with a high alert level, as well as connected face and recognition information is part of the area in *B*. There, also details of the face recognition and camera feed are expanded for further investigation by the analyst.

4 Collaboration

To allow analysts to work collaboratively in the dynamite environment, we introduce mobile-sandboxes as an extension of the three level workplace concept. Each mobile-sandbox, e.g. a smartphone or tablet, can be loaded with the current state of investigation, noteworthy snippets of data streams, or other important parts of the data. Analysts can use these devices to come together, exchange thoughts, and reason with the backing of data and parts of their very own workspace in a collaborative environment. Furthermore, each mobile-sandbox is capable of generating short, static reports, that can be transferred to any other sandbox or security personnel to exchange thoughts or facts from the data (streams).

5 Conclusions

The task driven design allows an arbitrary amount of investigators to efficiently exploit this tool. The overview uses intelligent aggregations of different streaming sources alerting its users in cases of suspicious events. This allows to start or proceed an investigation in form of tasks while staying alert in the overall environment. The HexaFlow streaming visualization supports the intuitive understanding of alertness and can be used for various streaming sources without the need to change the user experience. The adaptive detail screen as well as the mobile sandboxes grant a reporting environment and a bi-directive communication system useful for numerous people working in the casino.

Acknowledgments

This work was supported by the EU project VALCRI (FP7-SEC-2013-608142).

References

[1] J. Gehrke, F. Korn, and D. Srivastava. On computing correlated aggregates over continual data streams. In S. Mehrotra and T. K. Sellis, eds., *Proceedings of the 2001 ACM SIGMOD international conference on Management of data, Santa Barbara, CA, USA, May 21-24, 2001*, pp. 13–24. ACM, 2001. doi: 10.1145/375663.375665

[2] Y. Zhu and D. E. Shasha. Statstream: Statistical monitoring of thousands of data streams in real time. In *VLDB 2002, Proceedings of 28th International Conference on Very Large Data Bases, August 20-23, 2002, Hong Kong, China*, pp. 358–369. Morgan Kaufmann, 2002.