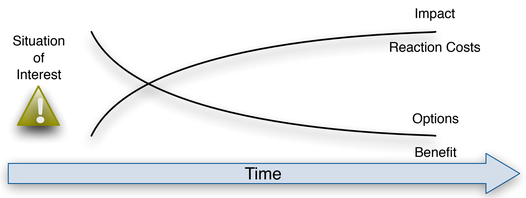
Anomaly Management using Complex Event Processing

Bastian Hoßbach and Bernhard Seeger
University of Marburg, Germany

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Introduction

Complex event processing (CEP) has emerged as a technological foundation for the continuous detection of situations of interest in near real-time. This allows to take action early. In this way, end-users become able to react on situations of interest optimally.



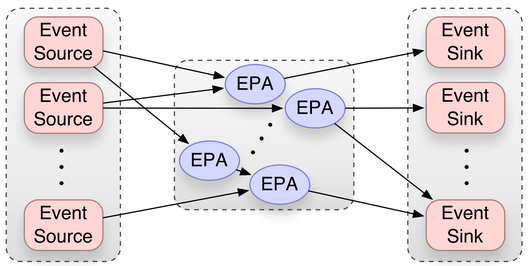
Problem Description

Current CEP infrastructures are static during runtime and not applicable in context-sensitive application domains:

- They are not adaptive to changes in the event flow
- Their event processing agents (EPA) are signature definitions and do not support anomaly management
- They are not reactive

Many application domains of CEP are dynamic, context-sensitive and require the management of anomalies, e.g.:

- Fraud detection
- IT-security
- Logistics
- Patient monitoring
- Stock market analysis



Static CEP infrastructures support:

✔ Signature-based monitoring

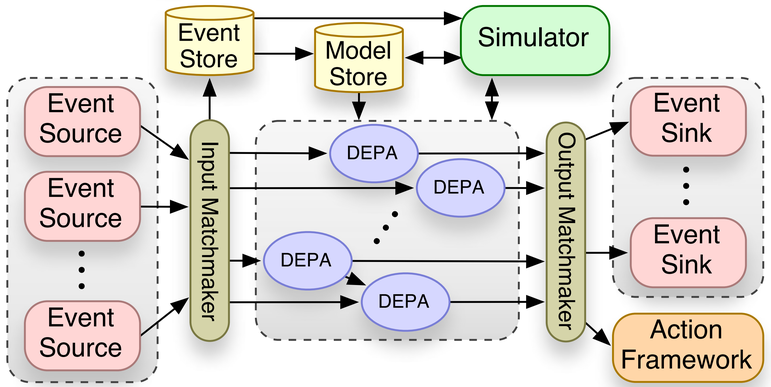
✘ Anomaly-based monitoring

Our Approach: Dynamic CEP Infrastructures

The event store is a high-performance database that records and indexes all events

The model store creates and maintains models that describe the application context and its changes based on historical data taken from the event store

The simulator is an isolated environment for testing, debugging and evaluating DEPA as well as context models on real event data



Matchmakers transform and route events dynamically at runtime and lead to independence between event sources and DEPA, DEPA and DEPA as well as DEPA and event sinks

Dynamic event processing agents (DEPA) are able to adapt to changes in the application context in a fast and safe way at runtime

The action framework triggers user-defined actions whenever a detected situation of interest fulfills the corresponding conditions

Additional Problems

Every CEP infrastructure that is built today depends heavily on the used CEP system, because there is no standardization. Due to different interfaces and query languages it is not possible to replace a CEP system by another one or to use different CEP systems within a federation.

The management of data quality is a big issue since the very first database systems have been developed. In CEP applications the roles of data and queries are reversed. Therefore, the management of the query quality becomes critical. At the moment, there are no tools, best practices and research that can be used to achieve a high quality of EPA.

Conclusion

State of the art CEP technology is static, inflexible, not reactive and does only support the signature-based monitoring paradigm. These shortcomings avoid the use of CEP in some important application domains and reduce the monitoring quality in many existing ones. Therefore, CEP technology has to be improved and extended in order to support other monitoring paradigms besides the signature-based one.

Acknowledgments

This work has been supported by the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung) under grant no. 16BY1206A.

Contact

Bastian Hoßbach
E-Mail: bhossbach@mathematik.uni-marburg.de
Phone: +49 6421 28 21575
Fax: +49 6421 28 21573

Bernhard Seeger
E-Mail: seeger@mathematik.uni-marburg.de
Phone: +49 6421 28 21526
Fax: +49 6421 28 21573