A Unified Framework for Detection of Suspicious and Anomalous Beahvior from Spatio-Temporal Traces

Boštjan Kaluža
Department of Intelligent Systems, Jozef Stefan Institute, Jamova cesta 39, Ljubljana, Slovenia
bostjan.kaluza@ijs.si, http://bostjankaluza.net

Thesis Summary

Keywords: agent, agent behavior, suspicious behavior, anomalous beahvior, anomaly detection

Received: June 10, 2014

This paper presents a summary of the doctoral dissertation of the author on the topic of learning patterns of agent behavior from sensor data.

Povzetek: Članek predstavlja povzetek doktorske disertacije avtorja, ki obravnava temo učenja vzorcev obnašanja agenta iz senzorskih podatkov.

1 Introduction

The problem of learning behavior patterns from sensor data arises in many applications including smart environments, video surveillance, network analysis, human-robot interaction, and ambient assisted living. Our focus is on detecting behavior patterns that deviate from regular behaviors and might represent a security risk, health problem, or any other abnormal behavior contingency. In other words, deviant behavior is a data pattern that either does not conform to the expected behavior (anomalous behavior) or matches previously defined unwanted behavior (suspicious behavior). Deviant behavior patterns are also referred to as outliers, exceptions, peculiarities, surprise, misuse, etc. Such patterns occur relatively infrequently; however, when they do occur, their consequences can be quite dramatic, and often negative.

We targets a large class of problems with complex, spatio-temporal, sequential data generated by an entity capable of physical motion in environment, regardless of whether the observed entity is human, software agent, or even robot. In such domains, an agent often has an observable spatio-temporal structure, defined by the physical positions relative to static landmarks and other agents in environment. We suggest that this structure, along with temporal dependencies and patterns of sequentially executed actions, can be exploited to perform deviant behavior detection on traces of agent activities over time.

2 Unified detection framework

We propose a unified framework to analyze agent behavior from prior knowledge and external observations in order to detect deviant behavior patterns. A detailed unified framework flowchart is outlined in Figure 1.

From the behavior analysis perspective, we propose a novel, efficient encoding that we refer to as a spatio-activity matrix. This matrix is able to capture behavior dynamics in a specific time period using spatio-temporal features, whereas its visualization allows visual comparison of different behavior patterns. Next, we provide a feature extraction technique, based on principal component analysis, in order to reduce the dimensionality of the spatio-activity matrix. We then introduce a clear problem definition that helps establish a theoretical framework for detecting anomalous and suspicious behavior from agent traces in order to show how to optimally perform detection. We discuss why detection error is often inevitable and prove the lower error bound, and provide several heuristic approaches that either estimate the distributions required to perform detection or to directly rank the behavior signatures using machine learning approaches. The established theoretical framework is extended to show how to perform detection when the agent is observed over longer periods of time and no significant event is sufficient to reach a decision. We specify conditions that any reasonable detector should satisfy, analyze several detectors, and propose a novel approach, referred to as a F-UPR detector, that generalizes utility-based plan recognition with arbitrary utility functions.

3 Empirical studies

The unified framework is demonstrated in three studies: detection of decreased behavior that indicates disease or deterioration in the health of elderly persons; detection of suspicious passengers in the airport simulation; and verification of persons at an access control point in high-security application.

The first study introduces an approach to monitoring an individual at home by an ambient-intelligence system to detect daily living pattern anomalies. It utilizes the pro-

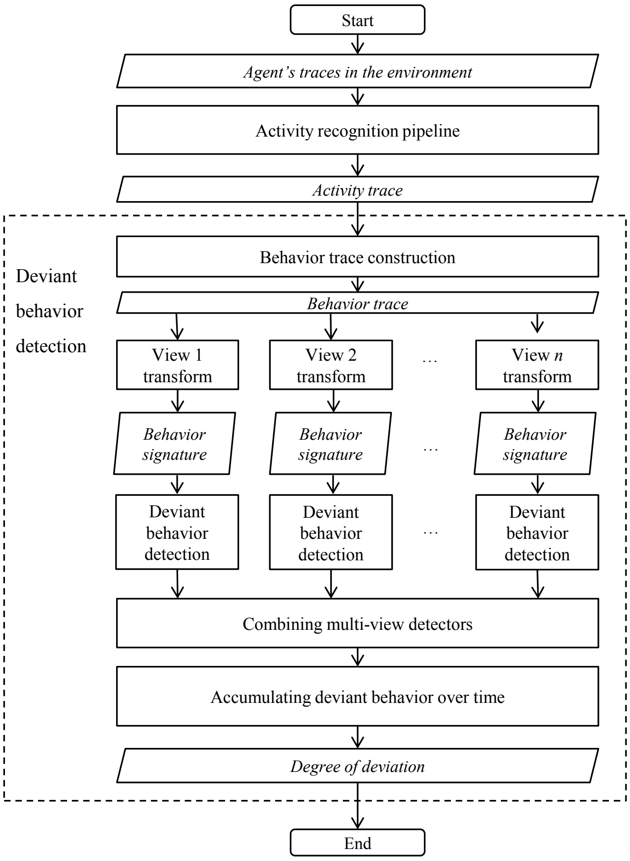
Start
Agent's traces in the environment
Activity recognition pipeline
Activity trace
Deviant behavior detection
Behavior trace construction
Behavior trace
View 1 transform
View 2 transform
...
View n transform
Behavior signature
Behavior signature
...
Behavior signature
Deviant behavior detection
Deviant behavior detection
...
Deviant behavior detection
Combining multi-view detectors
Accumulating deviant behavior over time
Degree of deviation
End

Figure 1: Processing flowchart of the unified framework.

posed unified framework to recognize activities, extract spatio-activity behavior signatures, and apply an outlier-detection method to classify the individual's daily patterns, regardless of the cause of the problem, be it physical or mental. Experiments indicate that the proposed solution successfully discriminates between healthy person behavior patterns and those of a person with health problems.

The second study focuses on two applications in surveillance domain, where the goal is to detect suspicious agents in the environment. In particular, it targets a large class of applications where no single event is sufficient to gauge whether or not agent behavior is suspicious. Instead, we face a sparse set of trigger events that identify interesting parts in behavior trace. The first application considers suspicious passenger detection at an airport, while the second application tackles dangerous driver detection.

The third study concerns entry control, which is an important security measure that prevents undesired persons from entering secure areas. The utilized unified detection framework allows an advanced risk analysis to distinguish between acceptable and unacceptable entries, based on several entry sensors, such as fingerprint readers, and intelligent methods that learn behavior from previous entries. First, it analyzes person behavior from different viewpoints and then performs a joint risk analysis. The obtained results represent an improvement in detecting security attacks.

In summary, we proposed a novel framework for suspicious and anomalous behavior detection, and demonstrated its applicability in three empirical studies.

References

[1] Kaluža, B. Detection of suspicious and anomalous beahavior detection from spatio-temporal agent traces. PhD thesis, Jozef Stefan International Postgraduate School (2013).

[2] Kaluža, B.; Gams, M. Analysis of daily-living dynamics. *Journal of Ambient Intelligence and Smart Enviroments* 4, 403-–413 (2012).

[3] Kaluža, B.; Dovgan, E.; Tušar, T.; Tambe, M.; Gams, M. A probabilistic risk analysis for multimodal entry control. *Expert Systems with Applications* 38, 6696-–6704 (2011).