

Research proposal for FORSEC

Huang Xiao

Institute of Informatics
Technische Universität München, Germany
xiaohu@in.tum.de

Abstract. A collection of research lines proposed by Huang Xiao.

1 Robust Anomaly Detection in Mobile Devices

The diverse and evolvable characteristics of anomalies in various scenarios prohibits the homogeneous development of a detection framework. For instance in the mobile devices, the rapid growth of different applications and services always comes along with a portion of novel attempts to compromise corresponding assets. The anomaly detectors can either neglect their existences or overreact to invoke false alarms on legitimate activities. Especially, mobile devices are highly correlated with users' own behaviors which requires that the robustness of the anomaly detection can bear the environmental complexity.

In this line of research, we concentrate on the complicate data patterns and also the essentials of state-of-art anomaly detection techniques [1,2], from which we develop a robust adaptation for mobile device. One possible application would be the secure payment transaction monitoring service. It monitors every payment transaction from the mobile device to prevent the unexpected financial loss. Instead of detecting the anomalies based on the payment information only, a robust detector also relies on the side information, such as the calendar, recent phone calls and also the supervision of user himself. The side information facilitates the monitoring routine to achieve its robustness.

References

1. A. Ben-Hur, D. Horn, H.T. Siegelmann, and V. Vapnik. A support vector clustering method. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, volume 2, pages 724–727 vol.2, 2000.
2. JooSeuk Kim and Clayton D. Scott. On the robustness of kernel density m-estimators. In *ICML*, pages 697–704, 2011.