inventions Geneva

2006 BU جامعة الباحة Al- Baha University

وزارة التعليم Ministry of Education

VISION رؤية 2030 المملكة العربية السعودية KINGDOM OF SAUDI ARABIA

InstaMon PackCap: On-the-fly Learning-powered Traffic Capturing Agent

Abstract

InstaMon PackCap is an agent as a specialized network device and software application designed to discreetly monitor network traffic without interfering with its flow. It employs and customizes the high performance capture engine and adopting brain-inspired hierarchical temporal memory (HTM) model named Simplified single cell assembled sequential hierarchical memory (s.SCASHM) to continuously learn the user traffic behavior within organization's network.

Introduction

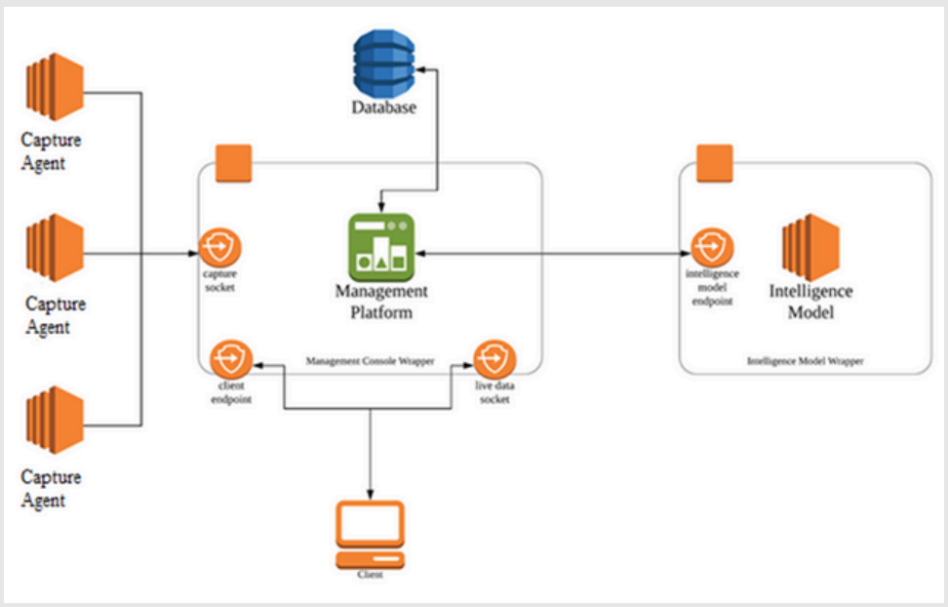
Cyber-attacks and threats are increasingly sophisticated and difficult to detect early. Attack patterns change rapidly, as such existing defense systems cannot recognize the patterns accurately. The systems require the ability perform on-the-fly learning on new attack patterns. Defending the inside from illegitimate user is challenging as the attackers enter through legitimate public ports then appears as just another user. This is the gap where we aim to fill with user behavioral analytics approach using the brain-inspired hierarchical temporal memory (HTM) models. Moreover, modern networks have huge bandwidth capacities, resulting high packet drop rates during packet tapping, which causes a decrease in the accuracy of the prediction engine. InstaMon PackCap combines the high performance capture engine and the s.SCASHM as on-the-fly learning model to improve the accuracy of the traffic prediction. InstaMon PackCap consists of 4 components, i.e.: Capturing device design, traffic capture process, Back-end data processing, and Historical data storage

Motivation

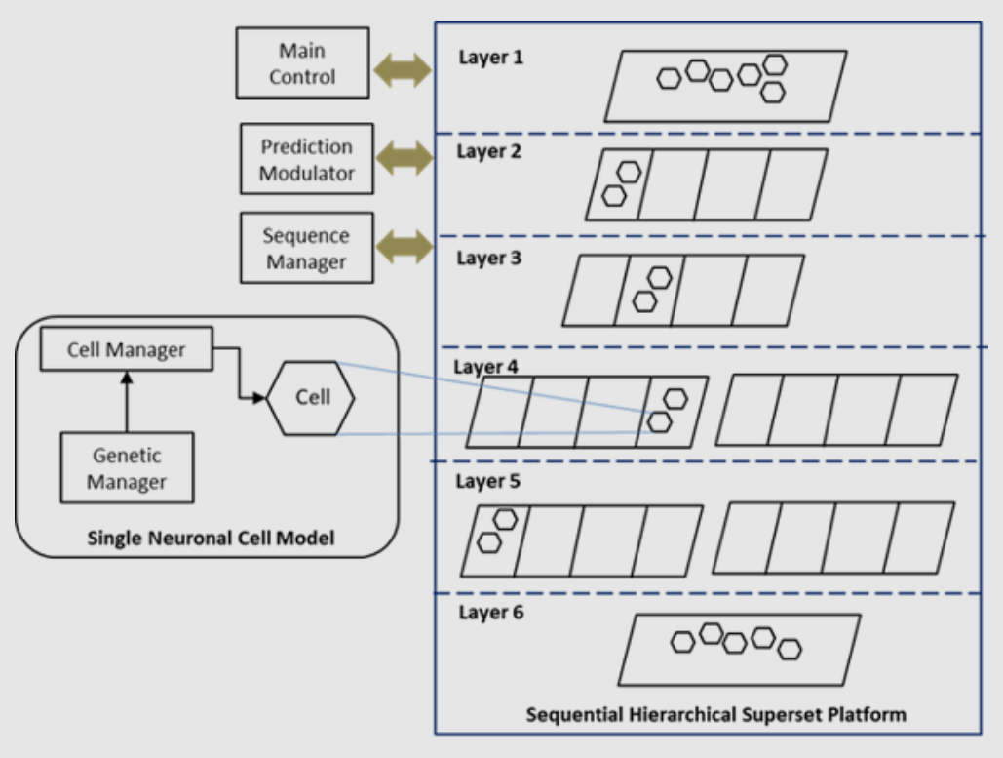
- Improve the accuracy of user's traffic behavior prediction.
- Increase the nation's cyber defense capability and resilience, through developing more cyber security tools locally.

Methodology

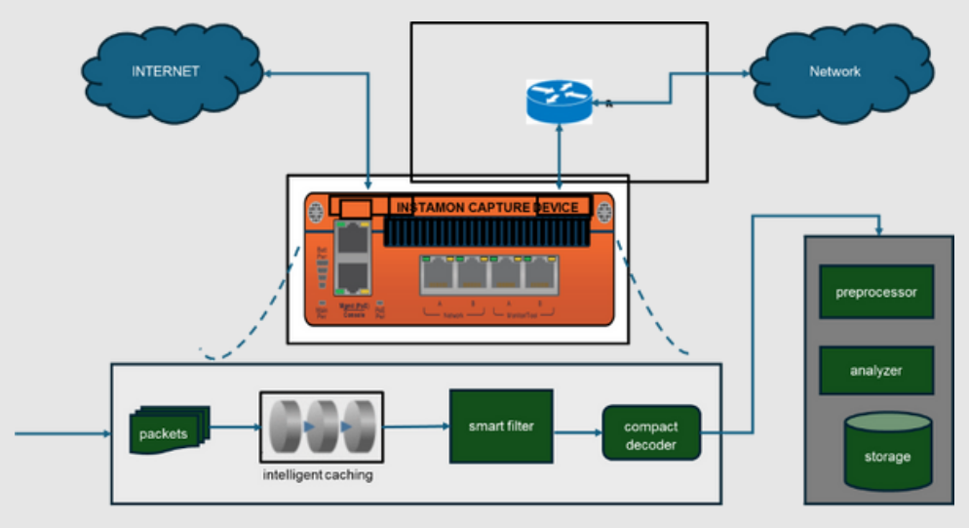
- Overall Proposed Method



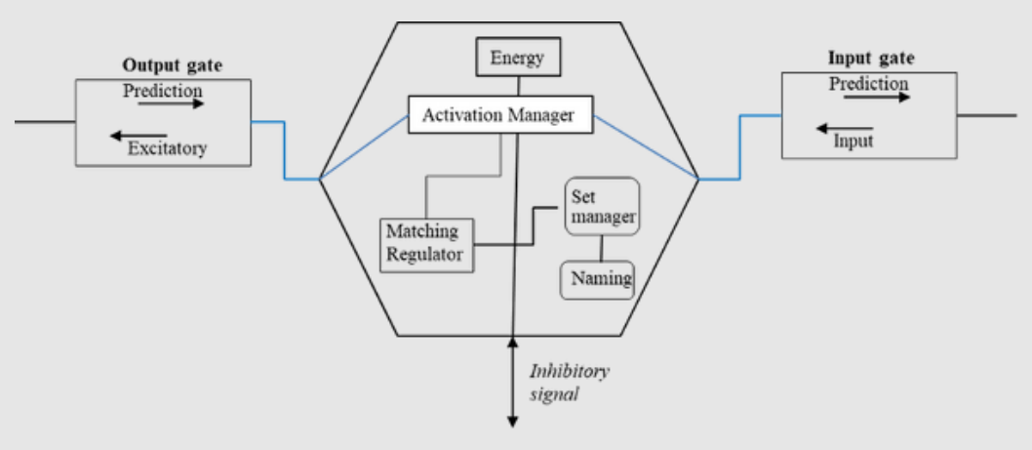
- The Sequential Hierarchical Superset (SHS) Platform.



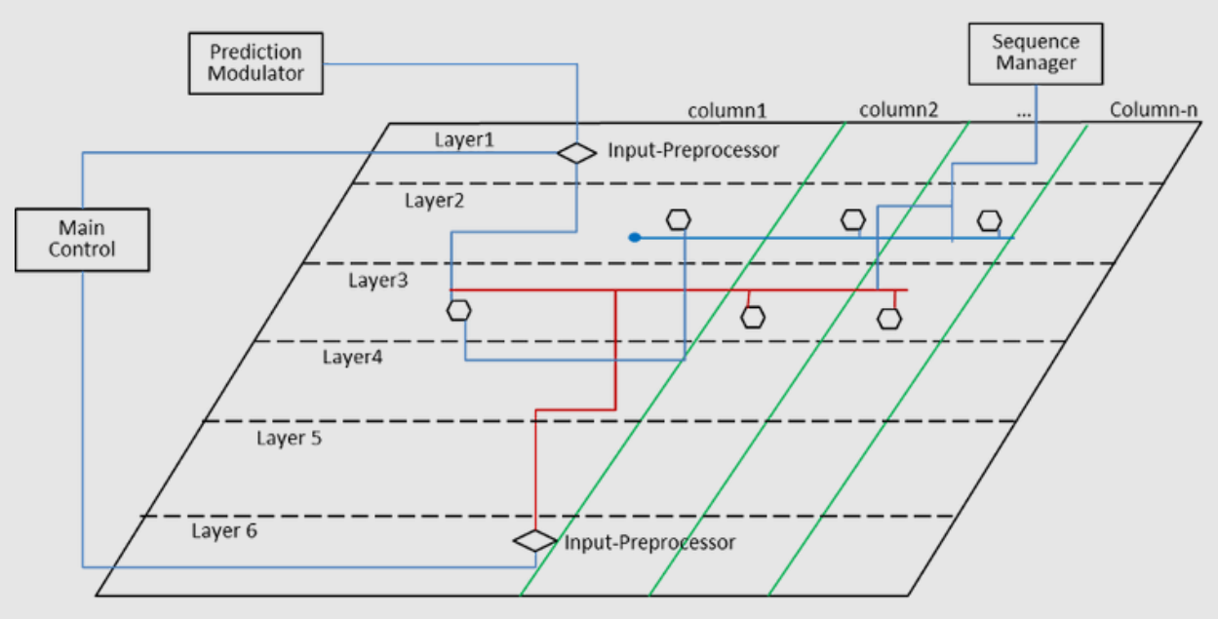
- The InstaMon PackCap



- I.Single Cell Neural Model

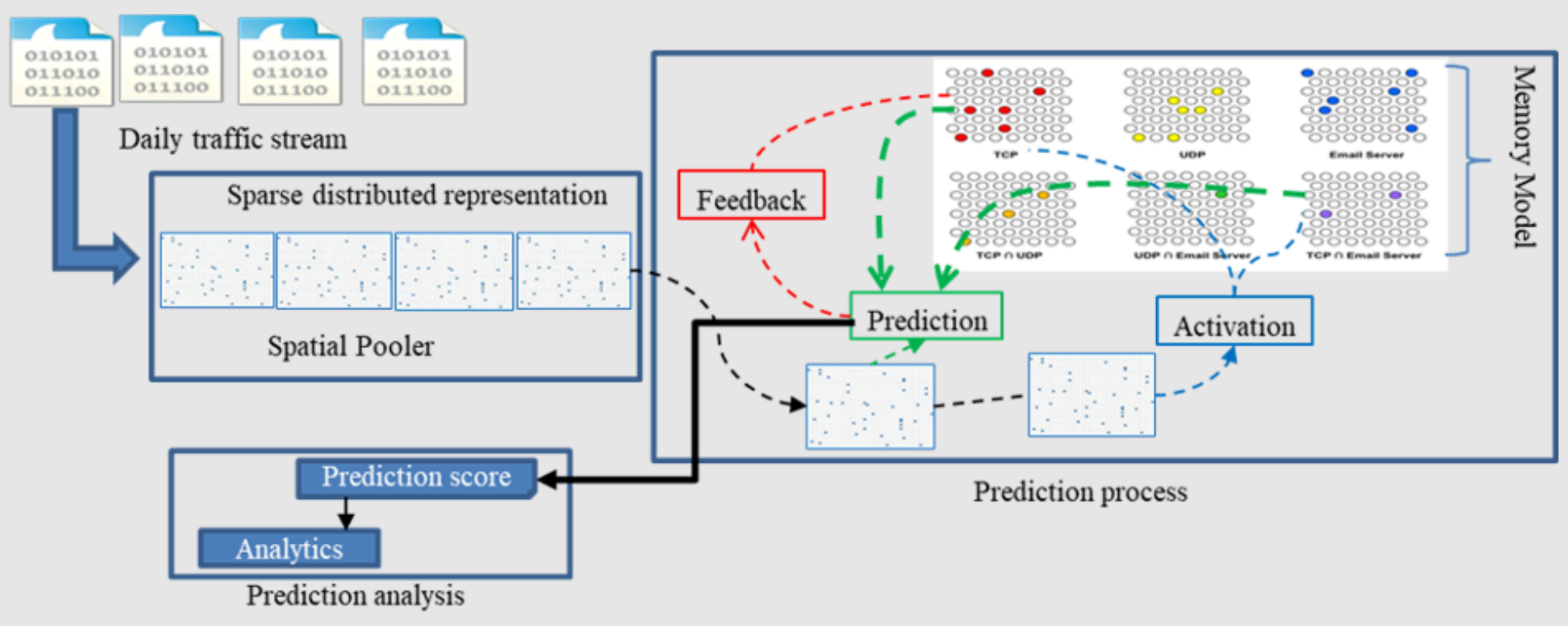


- s.SCASHM Model



Applications

Implementing the s.SCASHM for Intelligent passive headless real time packet capturing agent to support on-the-fly learning of network monitoring system



Contact

وزارة التعليم
Ministry of Education

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

المملكة العربية السعودية

Saudi Arabia