SEcure Cloud computing for
CRitical Infrastructure IT

Impact of Intra-cloud Live Migration on Anomaly Detection

Noor Shirazi
Steven Simpson
David Hutchison

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

SEVENTH FRAMEWORK PROGRAMME

Abstract

- Investigated the impact of live VM migration on state-of-the-art anomaly detection techniques, under various attack types and intensities.
- Key Findings :
  - Performance for AD degrades as shown by their ROC curves when live migration is initiated while VMs are under an attack (NS/PS/DoS) [1].
  - Presence of mgiration affects the ability of both techniqus to detect netscan more than DoS.

[1]. Simpson.S, Shirazi.N, Hutchison.D, and Helge.B, "Anomaly detection techniques for cloud computing," Dec. 2013. [Online]. Available: https://www.seccrit.eu/upload/D4-1-Aomaly-Detection-Techniques-for-Cloud.pdf

Intro: Anomaly detection

- Selection of AD techniques
  - Principal component analysis [Lakhina et.al]
  - Clustering based techniques (K-means) [Wu and Zhang]
  - Naïve Bayesian [Muda et.al]
  - Expectation Maximization (EM) for Gaussian Mixture Model (GMM) – EMGM [Markou and Sameer]
- Reasons
  - Ease of implementation
  - Proven ability to detect anomalies
  - Type of data
- For cloud computing
  - Lack of comprehensive comparison of existing methods
  - Lack of annotated datasets for their evaluation

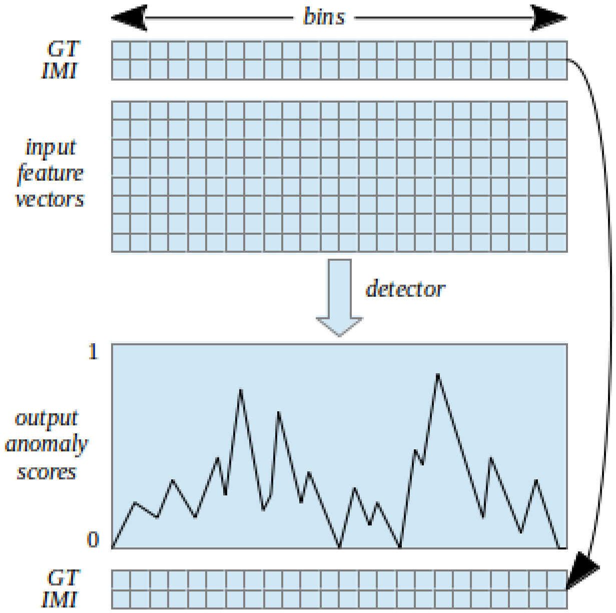
Intro: Anomaly detection

SEcure Cloud computing for CRitical infrastructure IT

- **Selection of Features**
  - Number of packets
  - Number of bytes
  - Number of active flows in each bin
  - Entropy of source IP address
  - Entropy of destination IP address
  - Entropy of source port
  - Entropy of destiation port
  - Entropy of packet size

- **Evaluation metrics**
  - Anomaly score graph (ASG)
  - Detection rate
  - ROC/PRC

- **Attack types**
  - Portscan , Network scan & Denial-of-service

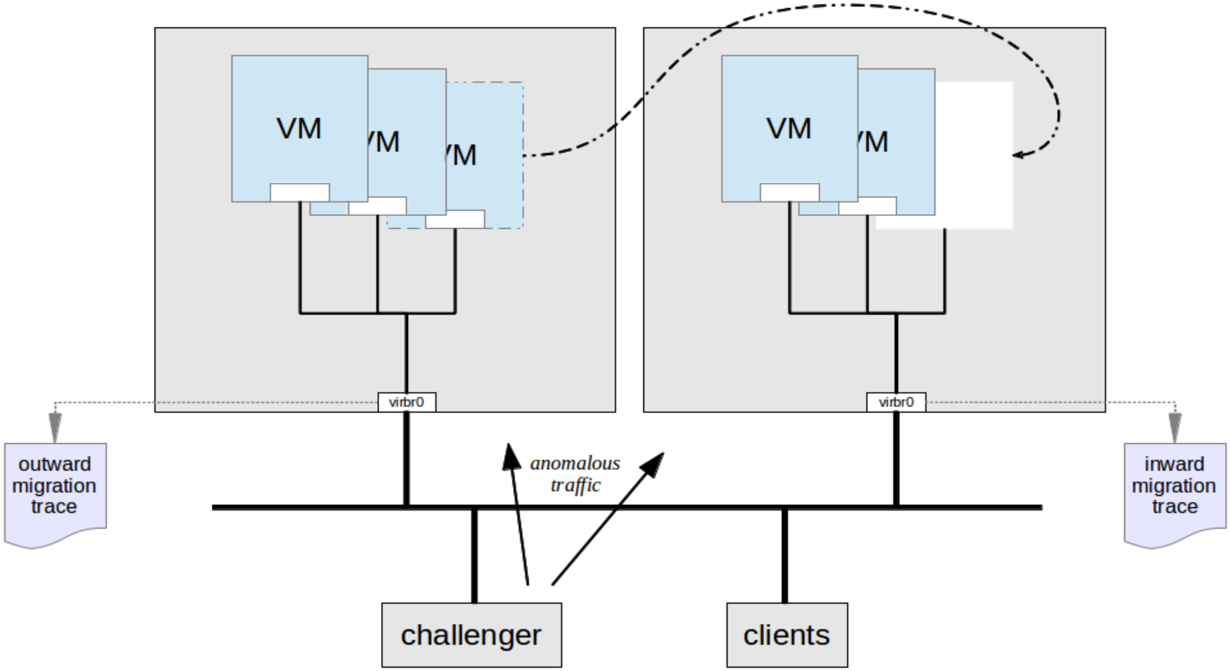


Evaluation framework

- The AD evaluation framework compose of various pre and post processing modules, which comprises of several scripts and libraries written in perl, python, C and Matlab.
  - Attack scripts
    - Volume and non-volume based attacks
    - Rate limiting features
  - Monitoring scripts
    - Tcpdump based
  - Background traffic scripts
  - Summary extraction scripts
    - Convert traffic into normalized statistical properties on a per packet basis
    - Based on libpcap
    - Provide interface to detector
  - Detector scripts
    - Reconfigurable as per the parameters (such as components/dimensions, thresholds, normalization schemes etc)
  - Visualization Scripts
    - Compare anomaly score to threshold and plot ROC and PRC curve

Experimental setup

- KVM for virtualizaton
- QEMU for hardware emulation
- Managed using Libvirt3 enables VM migration

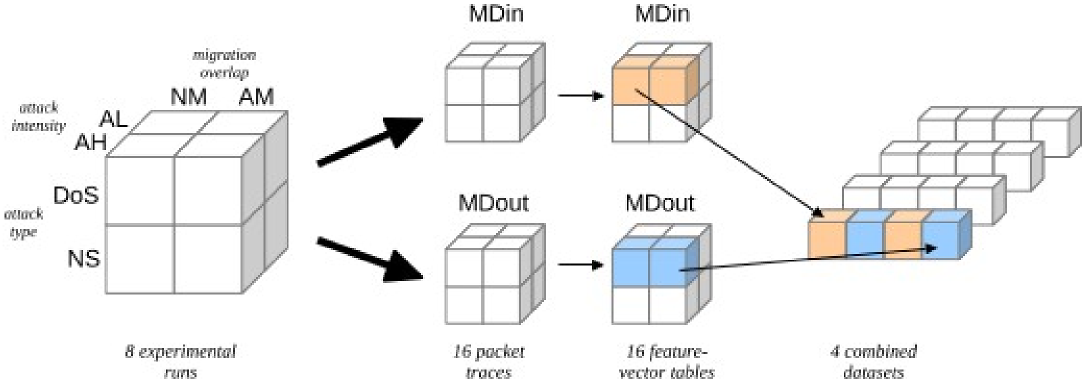


- Two physical VM hosts
  - Several VMs on each node running HTTPd
  - VM traffic logged
  - Bridged onto same network

- In each run:
  - Start anomalous traffic half-way through
  - Live local VM migration during either normal or anomalous period

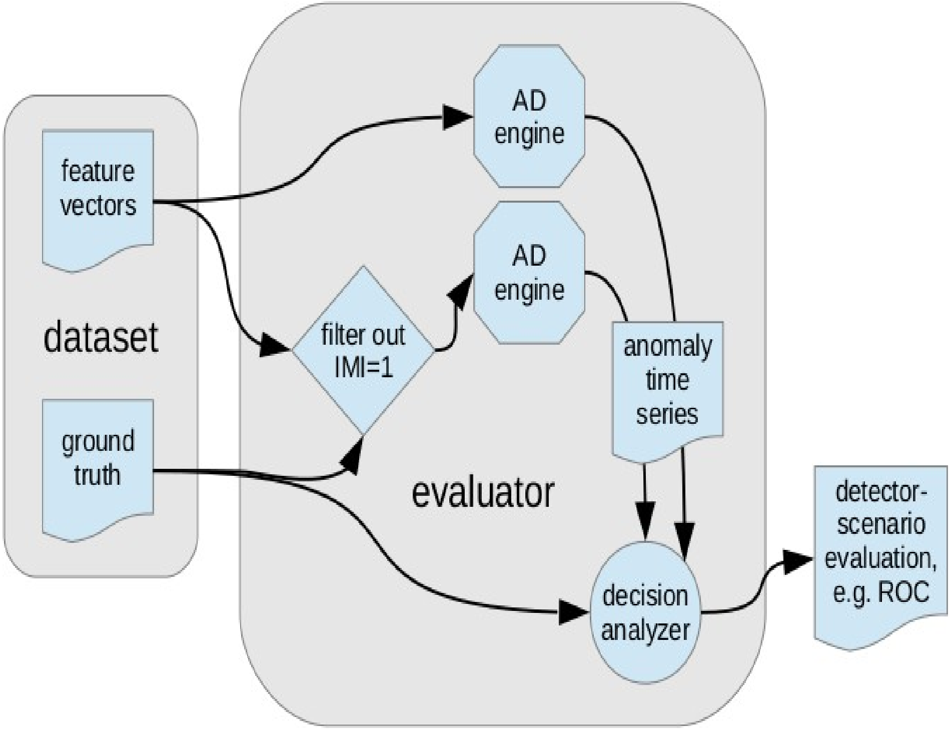
Evaluation method

- Experimental run yields packet traces with GT and IMI marked
- In each 10min run background traffic is at fixed rate.
- Attack scripts start 5 min, hence its traffic appears in each trace from the midpoint.
- At either 2.5 min or 7.5 min, a migration of one of the VM initiated.
- A run is characterized by attack type, intensity, migration overlap and node from which it was taken inward/outward
- Each trace is filtered to eliminate management traffic
- Divided into 1 second bins and each bin is convrted into feature vector from related traces. i.e the four in which the same atack type and intensity was applied with NM/AM and MDin/MDout varying., are combined to form a dataset



Evaluation process

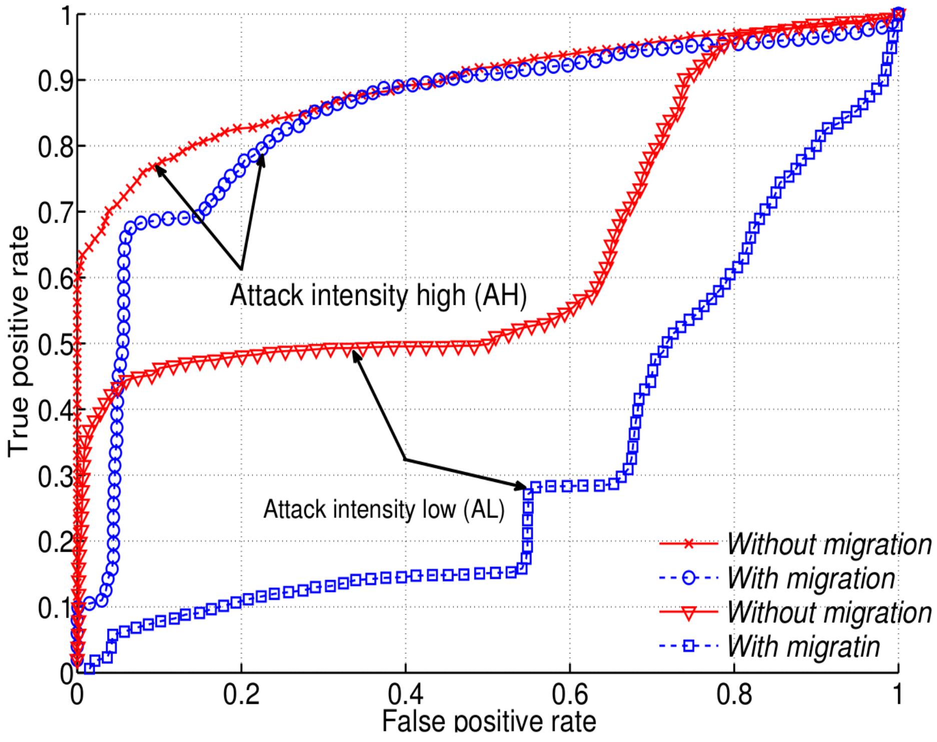
- Each examined detection technique is then appplied to each dataset by sumbitting them together to an evaluation process.
- Each dataset consists of a traffic trace and ground truth, and represents a scenario.
- An AD engine is instantiated according to an AD configuration.
- The traffic trace is fed into the engine to produce an anomaly time series
- The Decision Analyzer compares this series of probabilities with the binary ground truth for the equivalent period of time, and yields an evaluation of the AD configuration against the scenario.
- Partitioning the labeled output according to migration GT (IMI)
- Generate an evaluation of AD technique under both migration and non-migration situations



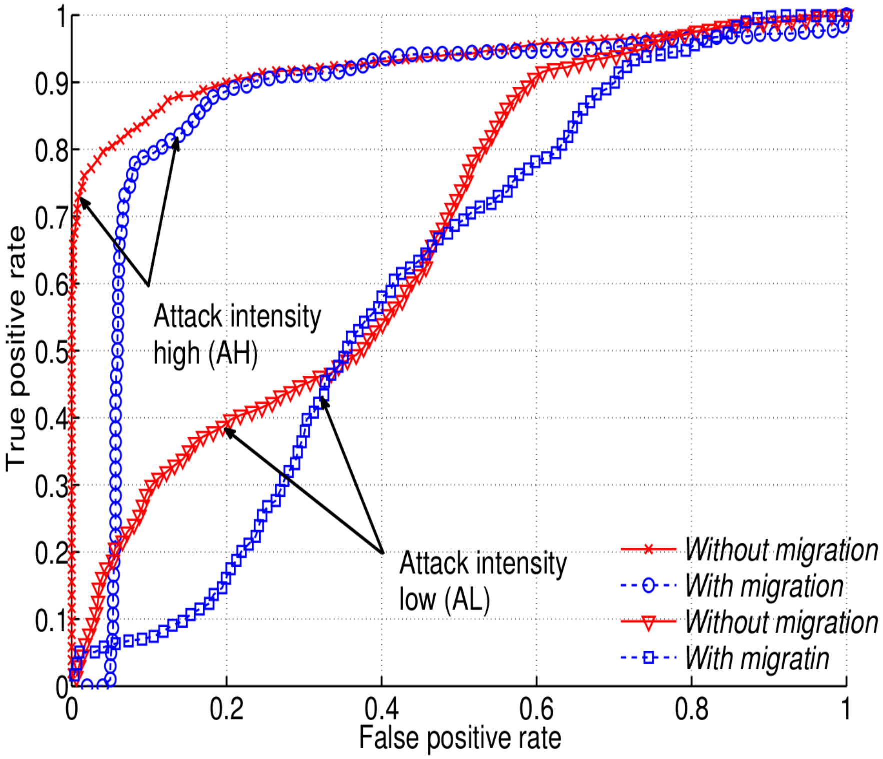
Results

- For more scenarios and experiments (refer to d4.1).

NS-AHAL-KM-ROC



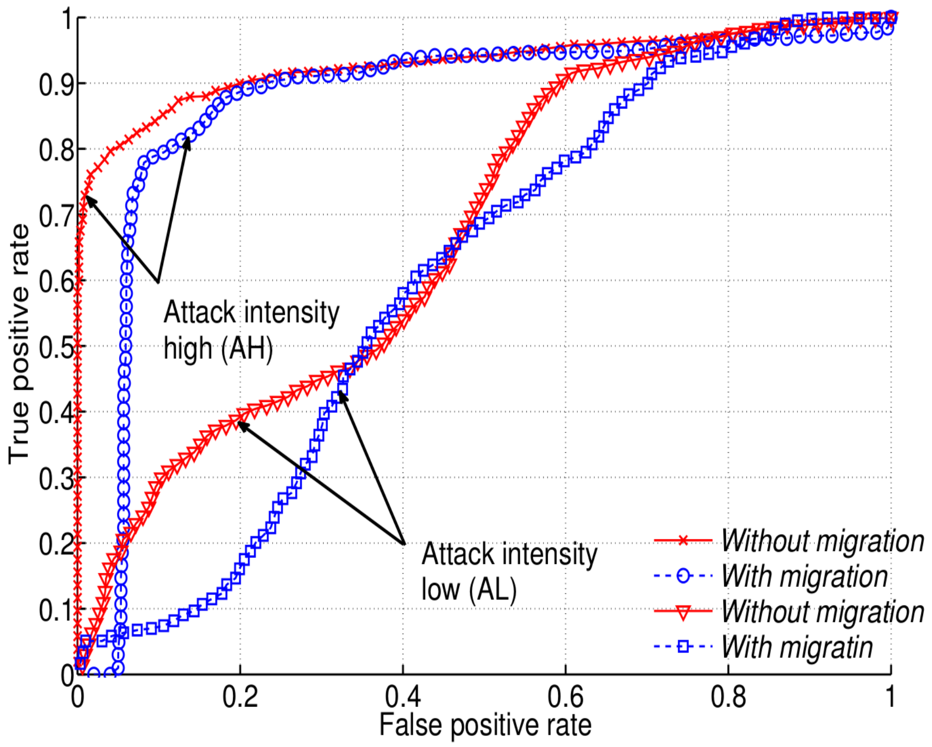
DoS-AHAL-KM-ROC



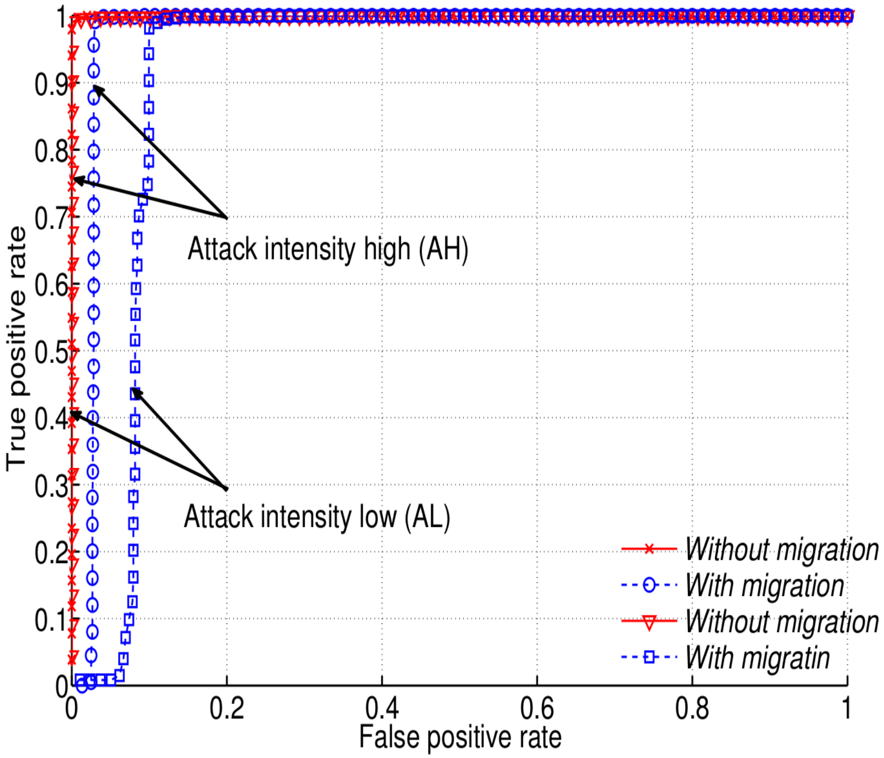
Results - cont

- For more scenarios and experiments (refer to d4.1).

NS-AHAL-PCA-ROC



DoS-AHAL-PCA-ROC



Conclusions

- We observed that migration has direct impact on performance of underlying AD control
- Future designs of cloud-oriented anomaly deteciton components should consider this factor.
- Unreliable for CI (high assurance services)

SEcure Cloud computing for CRitical Infrastructure IT

Contact

Noor Shirazi, Steven Simpson & David Hutchison

Lancaster University

n.shirazi@lancaster.ac.uk, ss@comp.lancs.ac.uk, d.hutchison@lancaster.ac.uk