CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

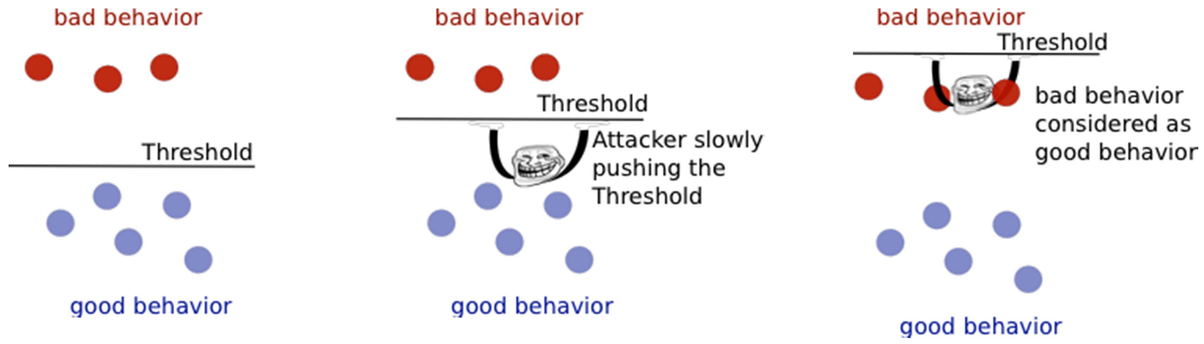
Securing Application-Level Topology Estimation Networks: Facing the Frog-Boiling Attack

Sheila Becker and Radu State
Interdisciplinary Centre SnT
University of Luxembourg

Jeff Seibert and Cristina Nita-Rotaru
Department of Computer Science and CERIAS
Purdue University

Frog-Boiling Attack:

Re-learning process of Intrusion Detection Systems abused to learn bad behavior as good behavior by gradually inserting small changes:



Goal of this work:

- Detecting frog-boiling attack
  - –Using supervised classification techniques
  - –Comparing CART, C4.5 and SVM
  - –For topology estimation networks – **Virtual Coordinate Systems**
  - –By defining appropriate feature set

Supervised Classification:

Why supervised? – We know how the system works; under normal updates; under malicious updates

Decision Trees

- Creation of rules:
  - –Mapping observations about the data to the class it belongs to.
- Classification and Regression Trees – CART
- C4.5

Support Vector Machines (SVM)

- Mapping input space into another dimensional space
- Kernel functions
- Render it linear separable

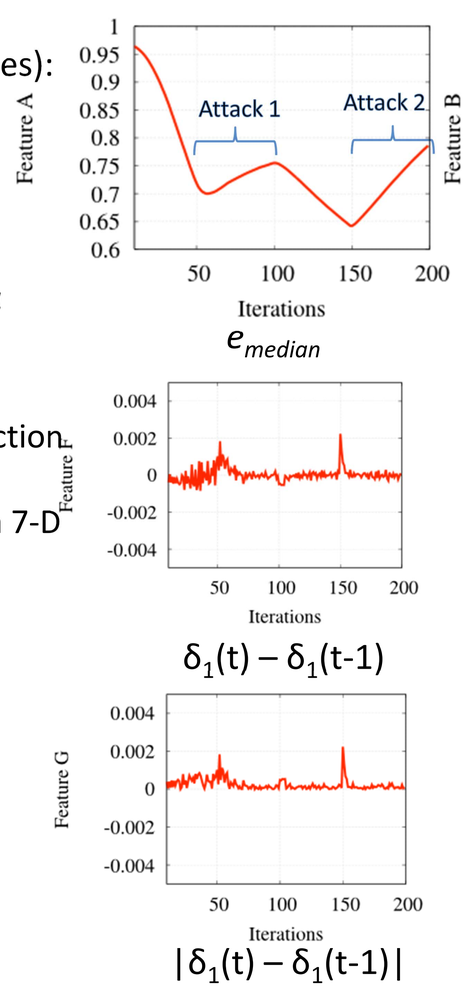
Virtual Coordinate System (VCS)

Performance optimization of P2P applications

- Nodes mapped into virtual coordinate space using synthetic coordinates.
- Nodes estimate latencies by calculating the distance between coordinates.
- **Vivaldi**: popular decentralized VCS, nodes are logically connected via a physical spring.
- Tension on the spring: if measured RTT ≠ estimated RTT. Nodes are updated accordingly.

The Challenge - Feature Set:

- Defining the right feature set (based on local error values):
  - –The raw data was not successful
  - –Simple time series values did not perform well
- We observed a four-lag correlation:
  - –Frog-Boiling: slow attack -> temporal correlation
    - Need to consider what happened at ***t, t-1, t-2, t-3, t-4***
    - Capture discretized form of second order derivate to indicate shape: $\delta_1(t) - \delta_1(t-1)$
    - Absolute value $|\delta_1(t) - \delta_1(t-1)|$ to get insight on inflection points.
  - –Decorrelate: embedding of the observed 1-D data into a 7-D manifold.



Results:

Attack Strategy	CART		C4.5		SVM	
	TPR	FPR	TPR	FPR	TPR	FPR
Frog-Boiling	0.96	0.05	0.97	0.04	0.80	0.21
Partition	0.93	0.04	0.93	0.03	0.83	0.17
Inflation	0.97	0.04	0.97	0.03	0.90	0.20
Deflation	0.99	0.02	0.98	0.02	0.90	0.21
Oscillation	0.99	0.02	0.99	0.01	0.95	0.10

CART and C4.5 outperform SVM
- High FPR for SVM

CERIAS

Discovery Park e-Enterprise Center