Activity Monitoring: Noticing Interesting Changes in Behavior

Foster Provost
New York University

ICML-2001
Williams College

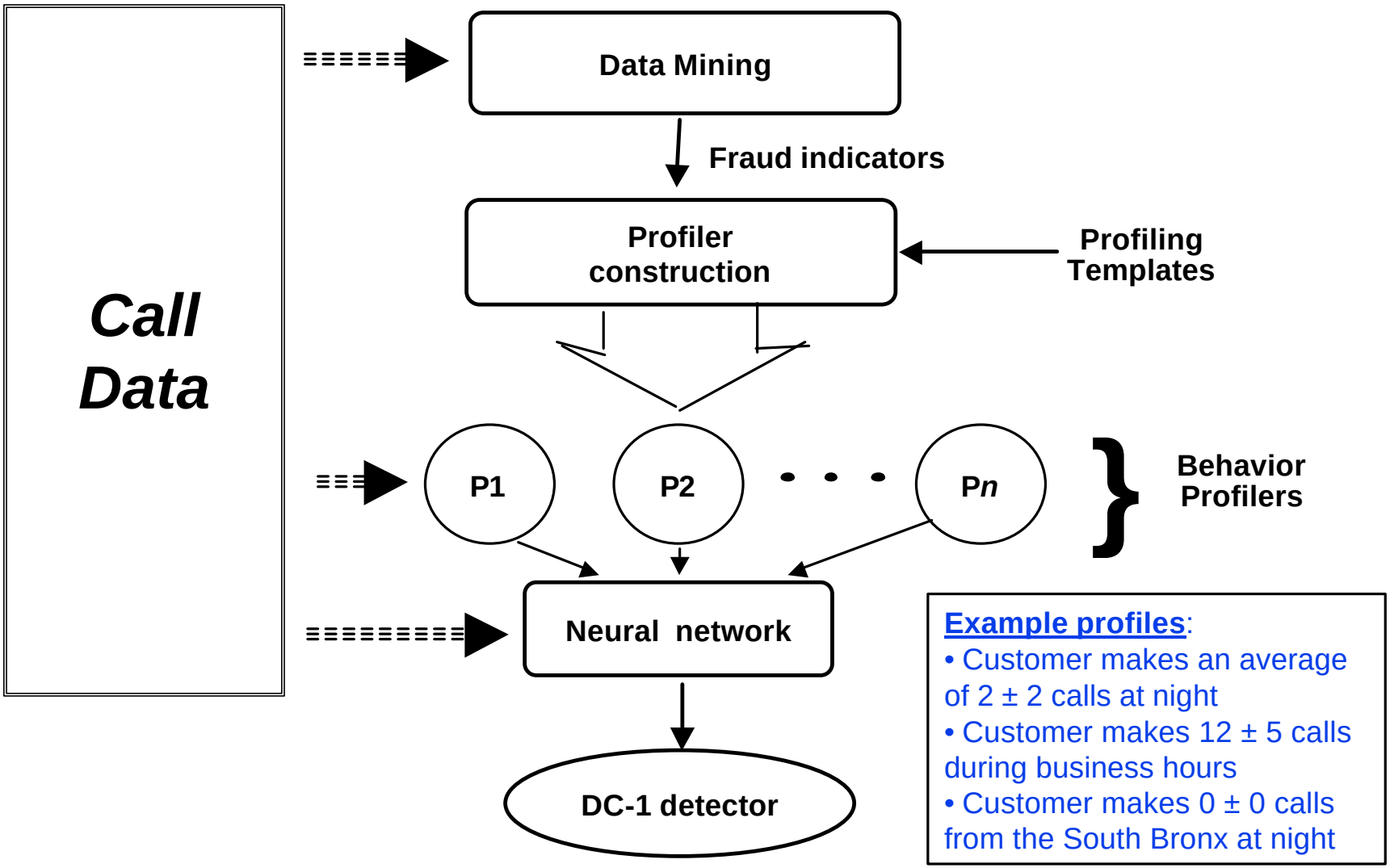
Fraud detection

Can we identify which accounts have been compromised so as to take corrective action?

A typical defrauded account

Date and Time	Day	Duration	From	To	Fraud
1/01/95 10:05:01	Mon	13 mins	Brooklyn, NY	Stamford, CT	
1/05/95 14:53:27	Fri	5 mins	Brooklyn, NY	Greenwich, CT	
1/08/95 09:42:01	Mon	3 mins	Bronx, NY	White Plains, NY	
1/08/95 15:01:24	Mon	9 mins	Brooklyn, NY	Brooklyn, NY	
1/09/95 15:06:09	Tue	5 mins	Manhattan, NY	Stamford, CT	
1/09/95 16:28:50	Tue	53 sec	Brooklyn, NY	Brooklyn, NY	
1/10/95 01:45:36	Wed	35 sec	Boston, MA	Chelsea, MA	YES
1/10/95 01:46:29	Wed	34 sec	Boston, MA	Yonkers, NY	YES
1/10/95 01:50:54	Wed	39 sec	Boston, MA	Chelsea, MA	YES
1/10/95 11:23:28	Wed	24 sec	White Plains,NY	Congers, NY	
1/11/95 22:00:28	Thu	37 sec	Boston, MA	EastBoston, MA	YES
1/11/95 22:04:01	Thu	37 sec	Boston, MA	EastBoston, MA	YES

Profiling customer behavior

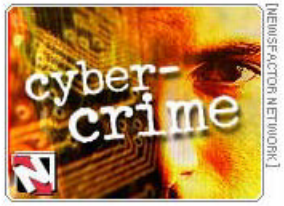


Example profiles:
- Customer makes an average of 2 ± 2 calls at night
- Customer makes 12 ± 5 calls during business hours
- Customer makes 0 ± 0 calls from the South Bronx at night

Ericsson Enlists AI To Fight Wireless Fraud

By Jay Wrolstad
Wireless NewsFactor
February 5, 2001

Send this Article | Related Stories
Print this Article | Talkback NEW!



Mobile network operators claim that 2 to 5 percent of total revenues are lost to fraud, and the problem is expected to worsen.

Artificial intelligence (AI) is the newest weapon in the fight against wireless phone fraud and theft, according to Swedish telecommunications giant Ericsson (Nasdaq: ERICY) and intelligent business systems company Searchspace Ltd. The two companies have joined forces to thwart individuals trying to cheat wireless network operators, Searchspace said.

Searchspace said its AI technology will be embedded in FraudOffice, Ericsson's telecommunications fraud management system, allowing the system to create phone usage profiles, learn from previous fraud examples and differentiate new forms of network and service abuse.

"Our technology provides a way to learn the best methods to detect fraud for any given operator by creating specific user profiles and identifying risk meaures and patterns of activity," Searchspace chief executive officer Konrad Feldman told Wireless NewsFactor.

In This Story:

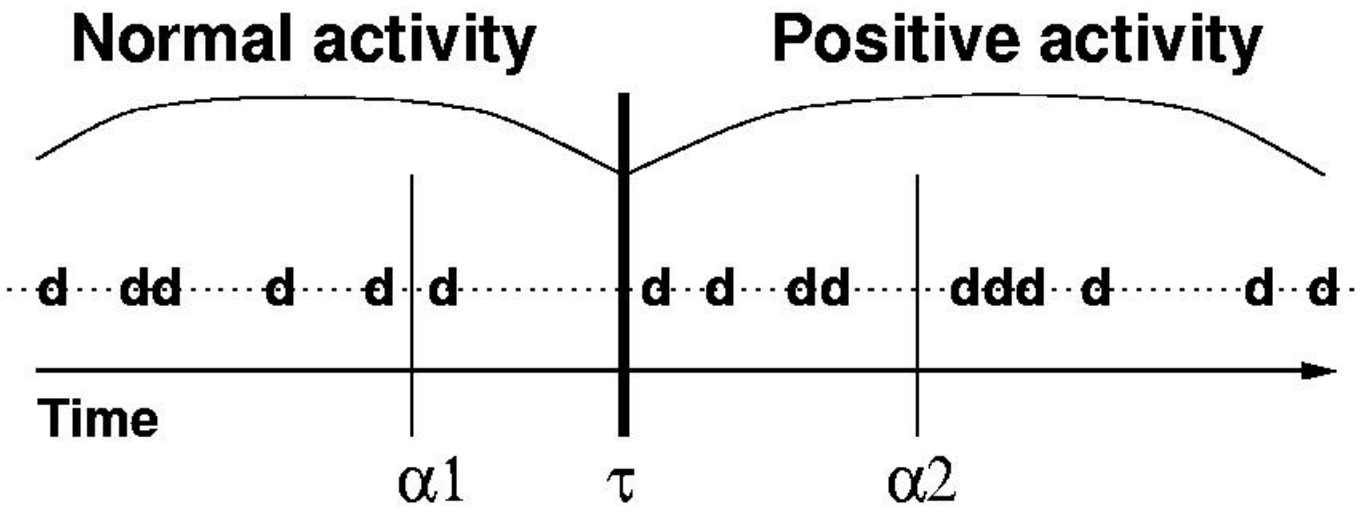
Creating User Profiles

Searchspace's technology monitors individuals' mobile phone use through intelligent plug-in software modules called sentinels, which create behavior profiles of network subscribers.

Those behavioral profiles include the types of calls made, the numbers called, the length of calls and when they are made.

According to SearchSpace, if suspicious activity on an account is detected, an alert is sent to the service provider, which in turn will employ an established response system to notify the

Activity Monitoring



τ = onset of positive activity

α1 = false alarm

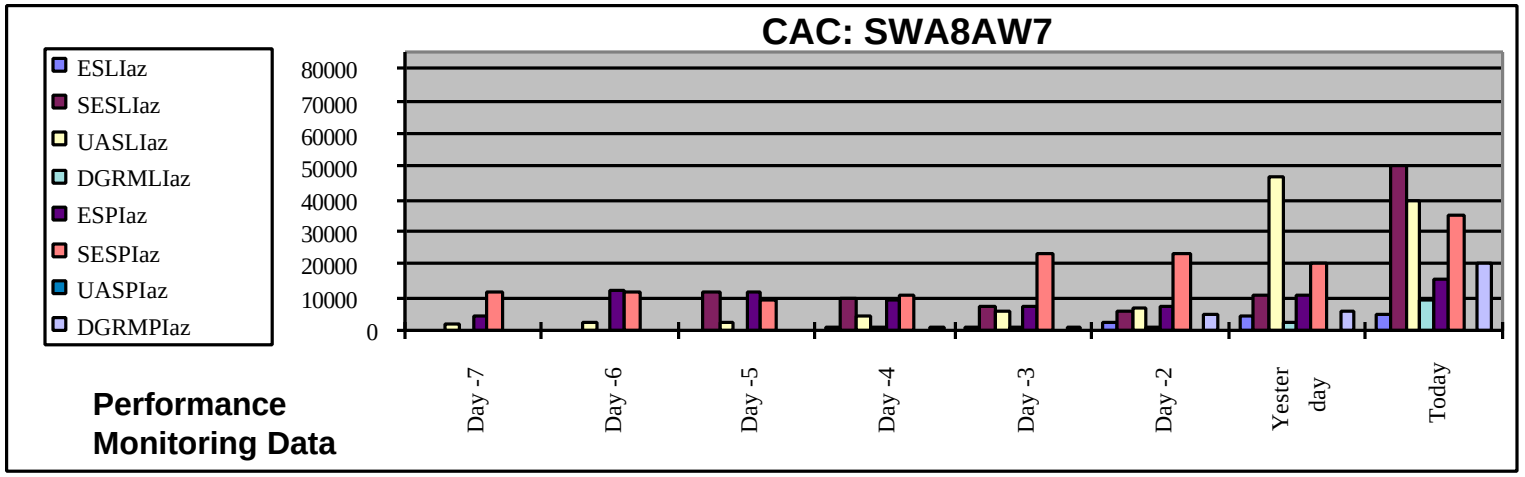
α2 = hit

Activity Monitoring tasks

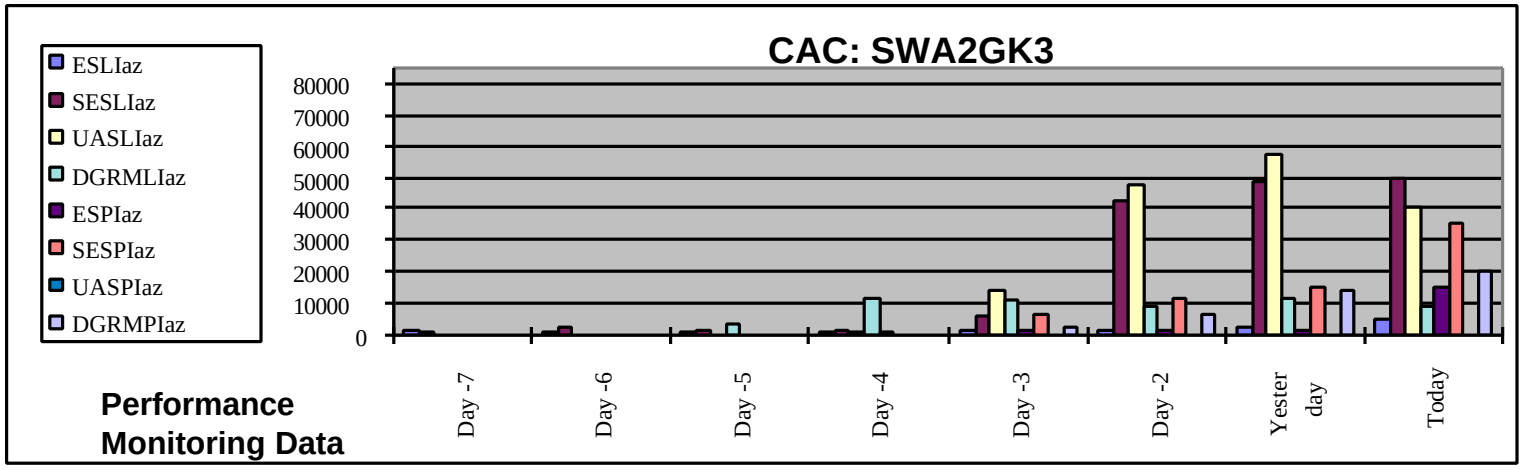
- Network performance monitoring
- Fault monitoring
- Crisis monitoring
- Financial market alerting
- Intelligent transaction monitoring
  - (e.g., for insider trading)
- Automated trading systems (e.g., for hedge funds)
- News alerting
- Intrusion detection
- Fraud detection
  - telecom, credit, insurance, etc.
  - note: fraud adapts to detection methods, so learning systems are essential

Predicting customer problems from performance monitoring data

For which CAC's is the likelihood of an impending trouble report highest?



trouble report?



trouble report?

Issues

- Multi-channel, multiple-type, time-sequence data
  - numerical, categorical, textual, feature-vectors, etc.
- Various possible granularities of data
  - different methods apply
  - coarser-grained summaries
  - comparative evaluation difficult
- Multiple alarm (don’t have equal value)
  - approximate formulations ignore this
- Timeliness of alarms is critical
  - delaying can be costly

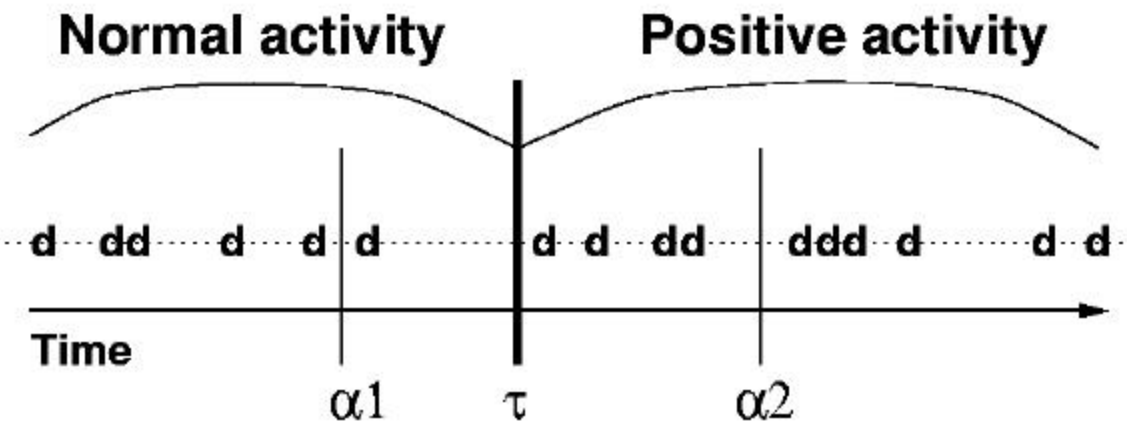
Activity Monitoring

Benefit of a hit?

$s(\tau,\alpha,H,D)$

Cost of a false alarm?

$f(\alpha,H,D)$



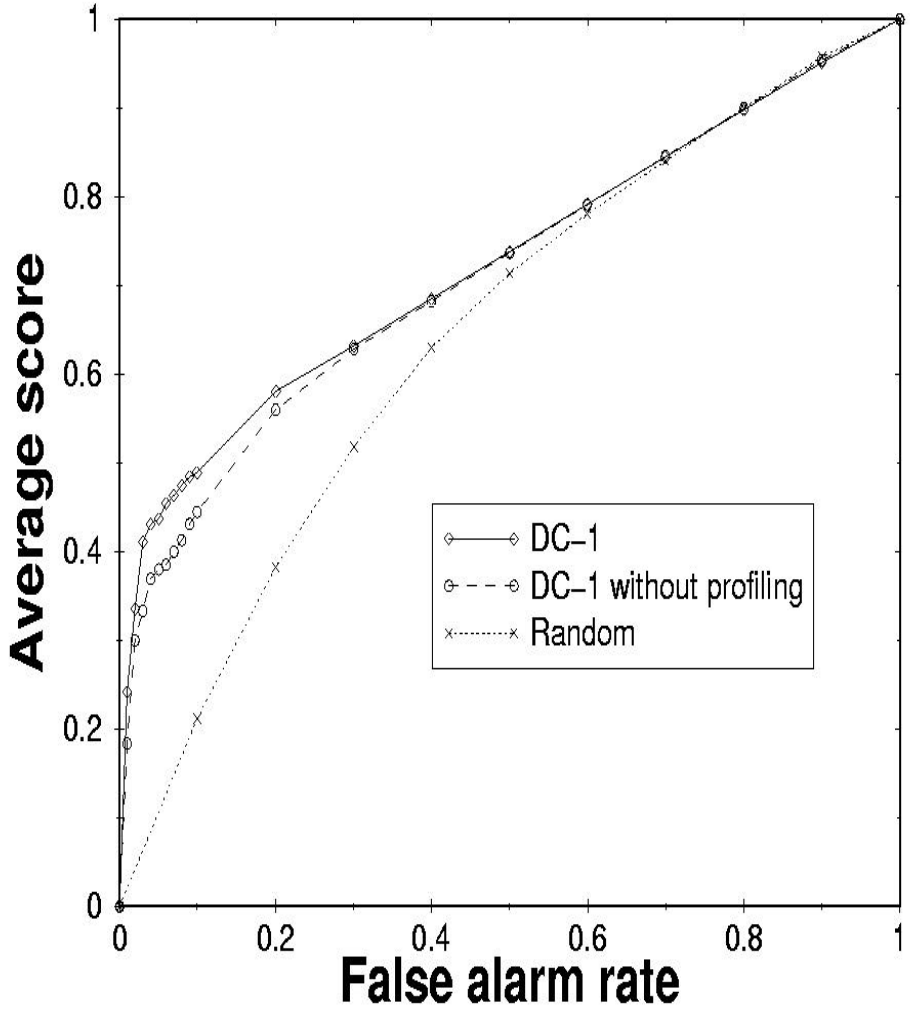
τ = onset of positive activity

α1 = false alarm

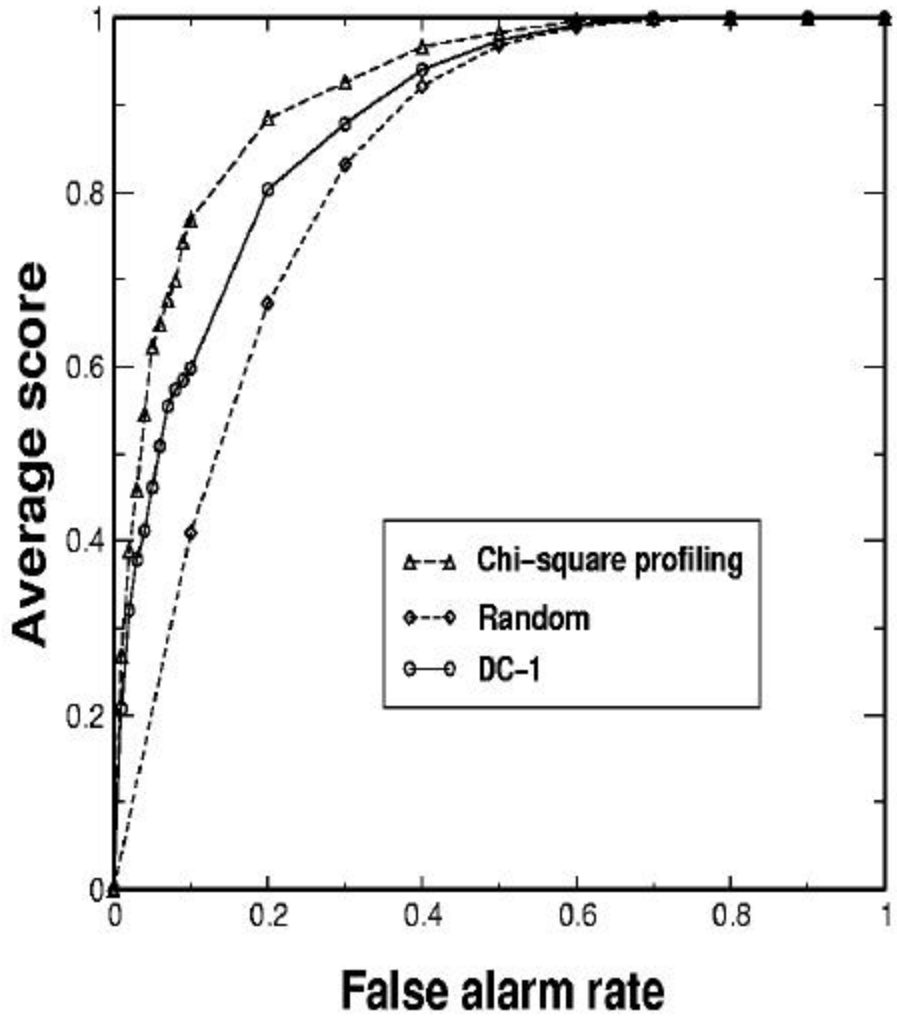
α2 = hit

Note: should normalize false alarms (per unit time)

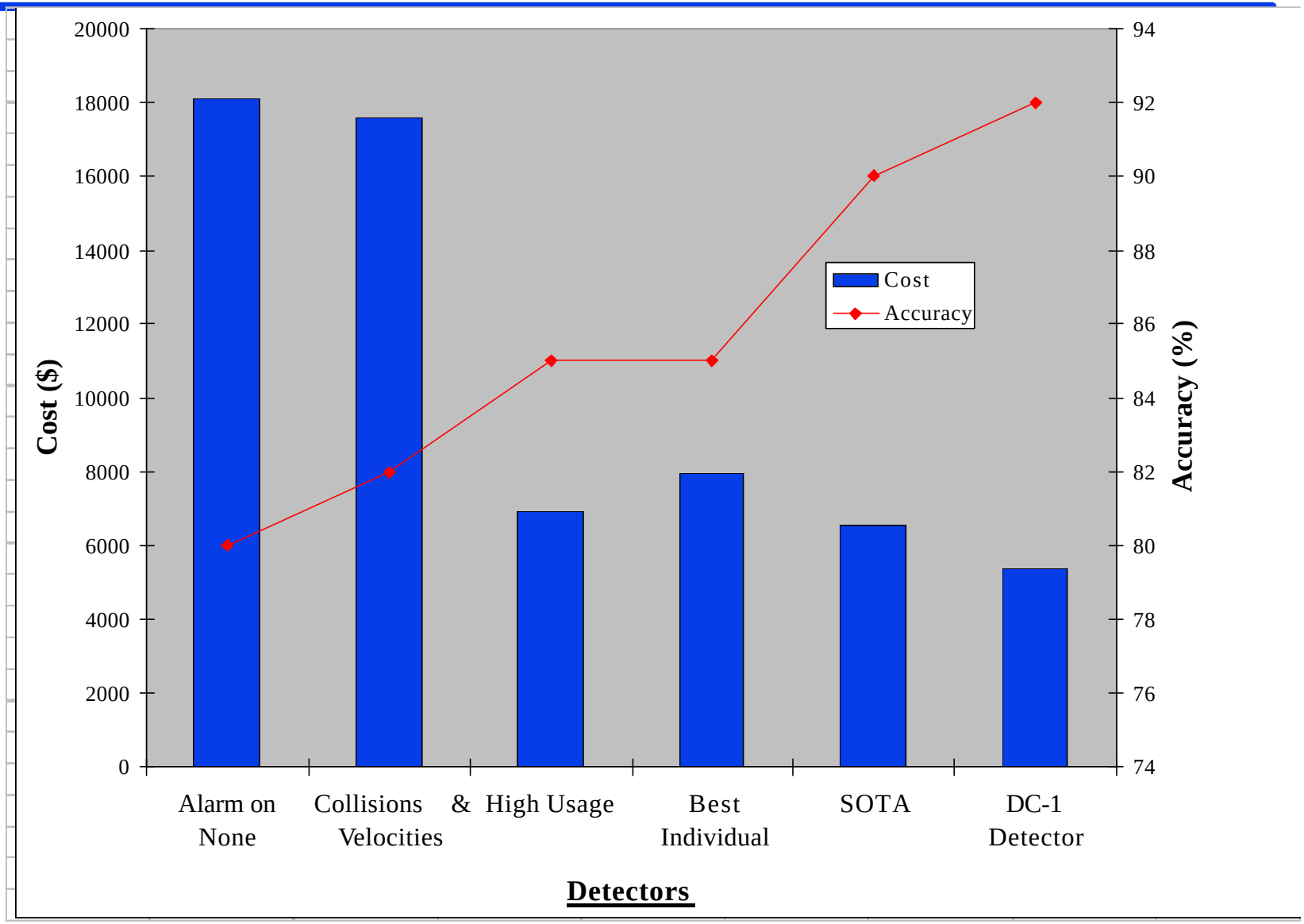
News Alerting



Intrusion Detection



Different methods for fraud detection



Activity Monitoring: Noticing Interesting Changes in Behavior

Foster Provost
New York University

The End

ICML-2001
Williams College