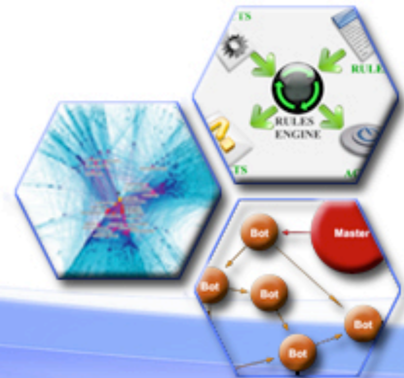
INFORMATION SECURITY CENTER OF EXCELLENCE

An Online Adaptive Approach to Alert Correlation

Hanli Ren, Natalia Stakhanova, and Ali A. Ghorbani

Information Security Center of eXcellence
University of New Brunswick
Fredericton, Canada



UNB

Outline

- Introduction
- Related Works
- System Overview and Techniques
- Implementation and Evaluation Results
- Conclusion and Future Work

Motivation

Problems:

- Traditionally IDSs generate a large number of alerts
- High percentage of false alarms

Potential solution:

- Alert correlation
    - *aims to build a high lever picture of the network security status.*

Challenges with alert correlation

- Two directions in alert correlation research:
  - *Knowledge Based Correlation*: reliance on expert knowledge
  - *Inference Correlation:* inference of relationships among alerts based on statistical or machine learning analysis.

	Strength	Weakness
Knowledge Based Correlation	1) high accuracy 2) explicitly show the logic relationship between the alerts	1) rely on expert knowledge 2) cannot correlate unknown attacks
Inference Correlation	1) do not need expert knowledge 2) detect unknown attacks	1) more time consuming 2) cannot explicitly show the causal relationship

Our approach

- The idea: bring together the strengths of expert knowledge-based and inference approaches for online alert correlation
  - *Similar to inference-based correlation*, we analyze the casual relationships among alerts using a Bayesian network and automatically extract the constraints and alert relationships that characterize attack steps.
  - *To provide better accuracy and ability to show the alert relationships* explicitly, we couple this analysis with network configuration information and expert knowledge.
  - *To ensure that unknown alerts* are considered we provide an adaptation mechanism during online analysis

- The proposed approach can be applied in
  - two stages: offline attack information extraction and online alert correlation.
  - one stage for post factum processing.

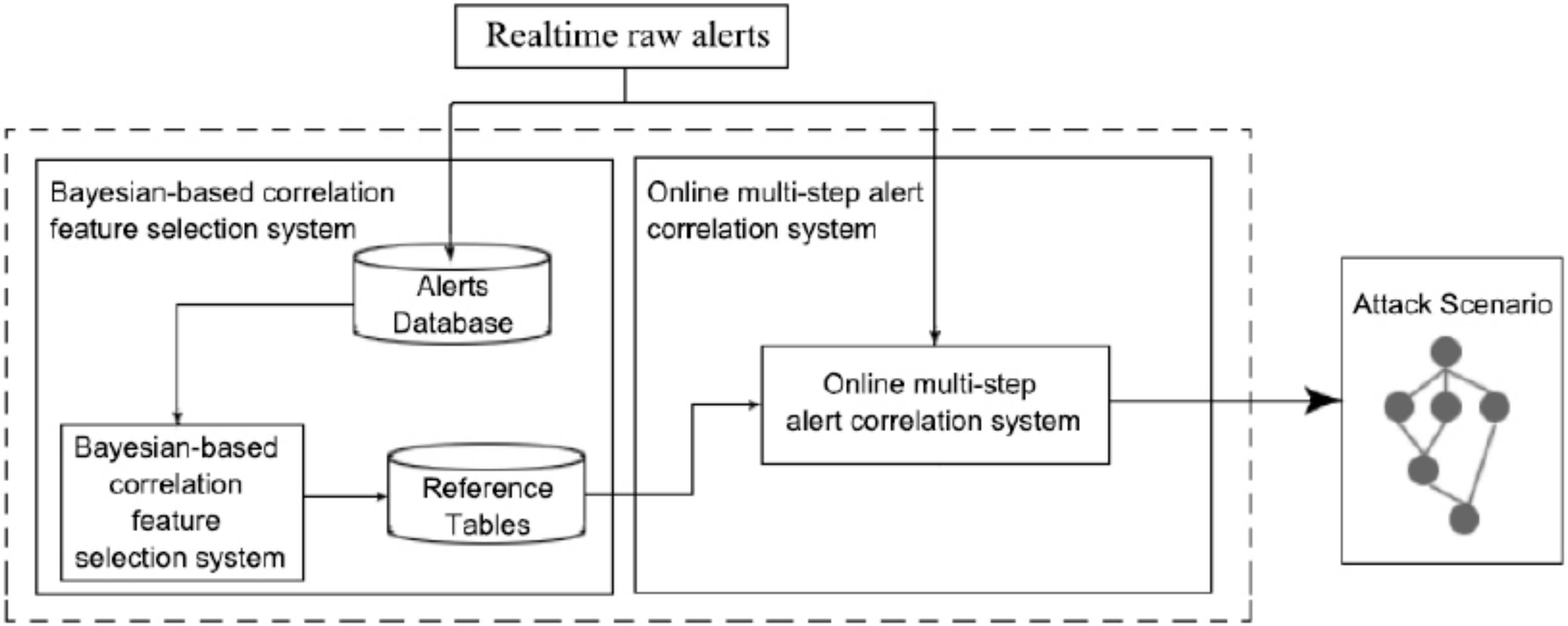
Our contributions

- **A Bayesian correlation feature selection model** that allows to automatically retrieve the causal relationships and relevant features among alerts without expert or domain knowledge.

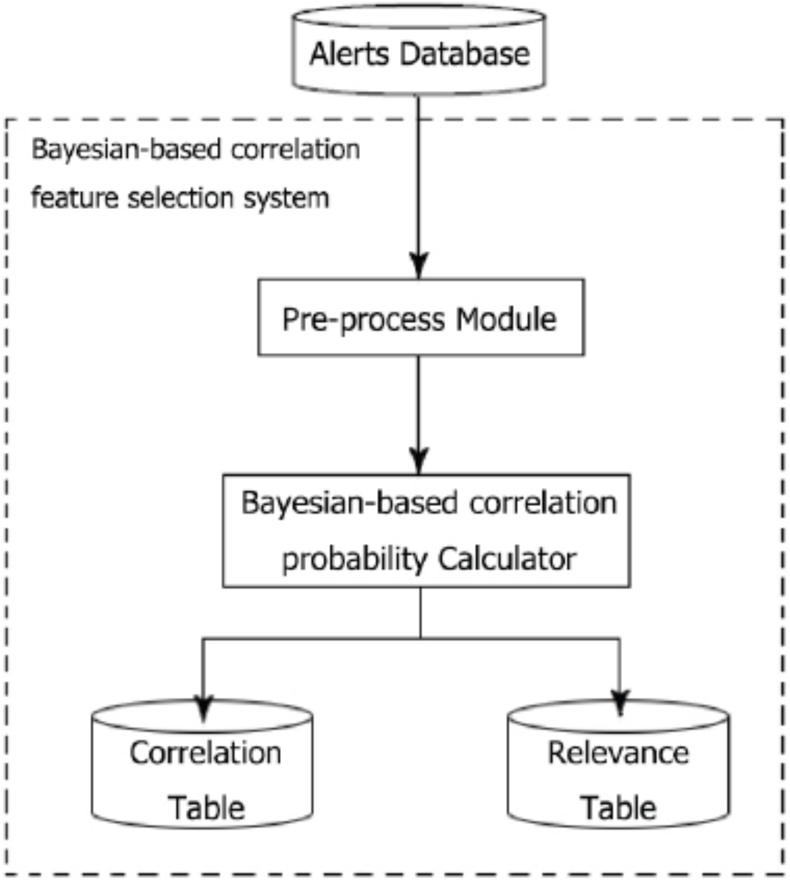
- **A method for online attack scenario construction** that allows a user to extract attack patterns and construct attack scenarios on-the-fly.

- **An implementation of the proposed approach**

System Overview



Offline component: Bayesian correlation feature selection system



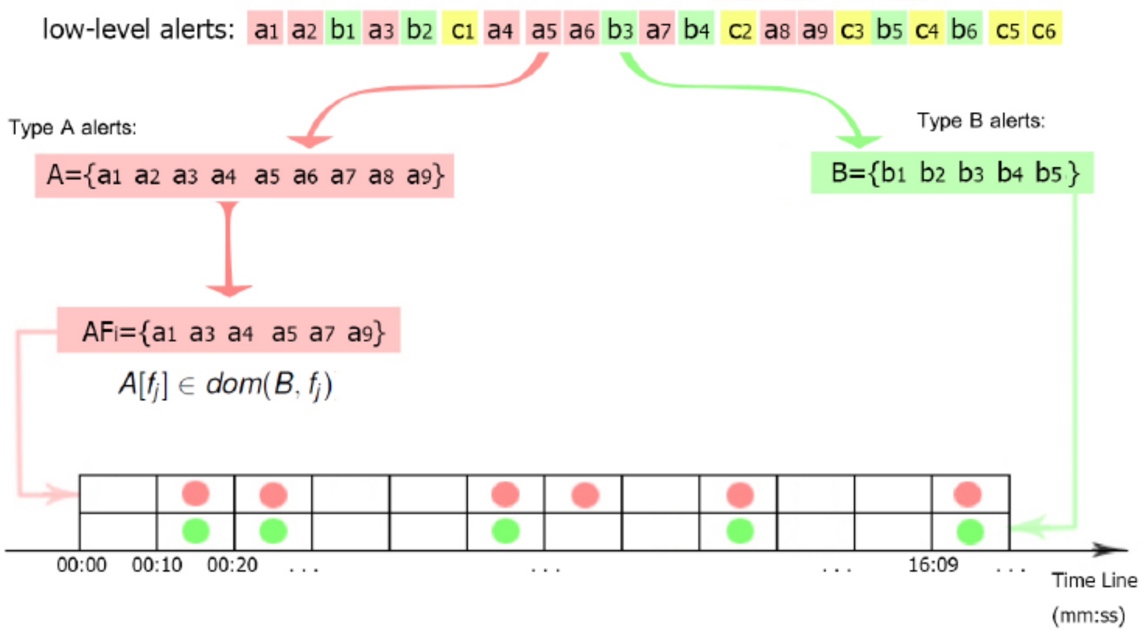
Step 1:
Standardize raw alerts, aggregate them based on alert types

Step 2:
Based on Bayesian causality, analyze the causal relationships between each alert type pair

Step 3:
Use a greedy algorithm to extract the features most relevant to the causal relationships

Output:
Correlation and relevance tables

Step 2: Apply Bayesian Causal Discovery to Alert Correlation



- $P(B|A[f_j] \in dom(B, f_j)) = P(B)$
  irrelevant feature
- $P(B|A[f_j] \in dom(B, f_j)) < P(B)$
  a relevant feature with negative influence
- $P(B) < P(B|A[f_j] \in dom(B, f_j)) < t$
  a relevant feature with positive influence
- $P(B|A[f_j] \in dom(B, f_j)) > t$
  a relevant feature with critical influence

Step 3: Most relevant features selection

- To select a subset of most relevant features, we use a greedy approach to analyze all possible combinations of features.

- Starting with pairs of features, the procedure randomly adds a feature to each subset whose probability exceeds the threshold.

Outputs of the offline component:

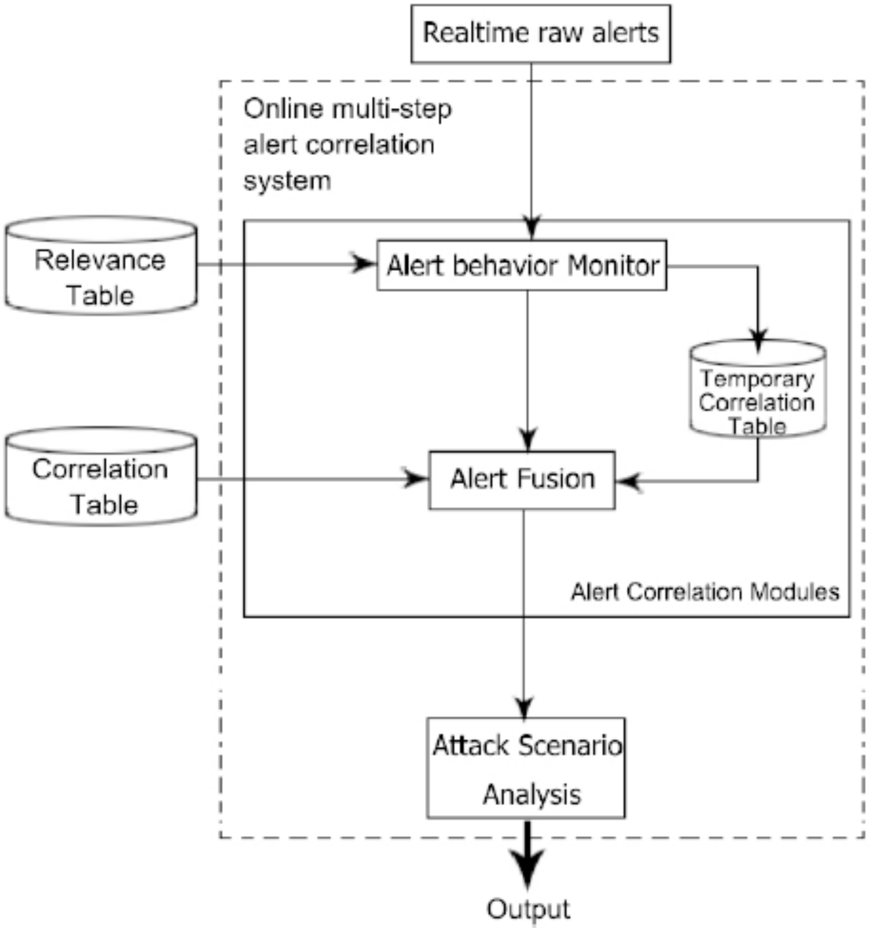
Correlation Table

Alert Type Pair	Correlation probability	Relevant Features
$< T_1.T_2 >$	70%	F2,F4,F6
$< T_1.T_3 >$	65%	F1,F3,F4,F6
...	...	...
$< T_2.T_5 >$	20%	F2

Relevance Table

Alert Type	OccProb of T_i Alerts	Relevant Alert Types	
		Strongly relevant	Weakly relevant
T_1	5%	T_2, T_3, T_5	T_4, T_7, T_8
...	...	...	...
T_i	10%	T_1, T_3, T_5	T_2, T_4, T_6
...	...	...	...
T_n	1%	T_7	T_1, T_2, T_3

Online component:
Multi-step Alert Correlation System



Step 1:
Standardize raw alerts

Step 2:
Monitor the occurrence probability of each type of alerts.
If there is any sudden change in the alert behavior, update the Temporary Correlation Table.

Step 3:
Correlate the alerts based on the information provided by both correlation tables.

Output:
Attack scenarios

An example of Correlation Process

Relevance Table

Alert Type	Occurrence Probability	Relevant Alert Types	
		Strongly	Weakly
A	54%		B,C
B	1%	C	A
C	45%	B	A

Step 1: calculate occurrence probabilitues

Alert Type	Occurrence Probability
A	40%
B	30%
C	30%

Step2: update Temporary Correlation Table

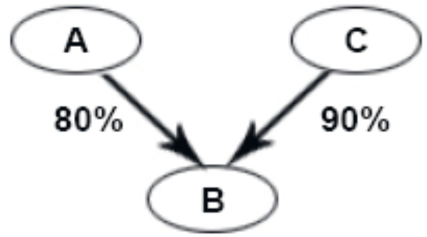
Temporary Correlation Table

Alert Type Pair	Correlation Probability	Relevant Features
<A,B>	80%	SrcIP

Correlation Table

Alert Type Pair	Correlation Probability	Relevant Features
<A,B>	10%	
. . .	. . .	. . .
<C,B>	90%	DesIP

Step3: build attack scenario



Experimental Results

We used following datasets to test the function and performance of the proposed approach:

- DARPA 2000 data set → function of the offline correlation module
  - *Experimented with LLDOS 1.0 scenario which includes a distributed Denial-of-Service (DDoS) attack*

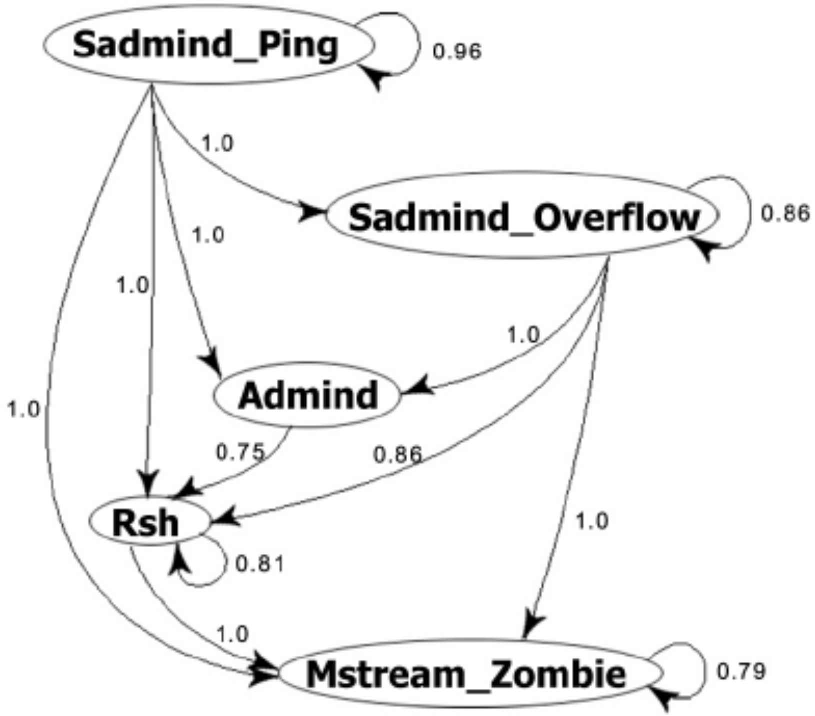
- Honeynet traffic → function of the online correlation module.
  → performance of the proposed framework.

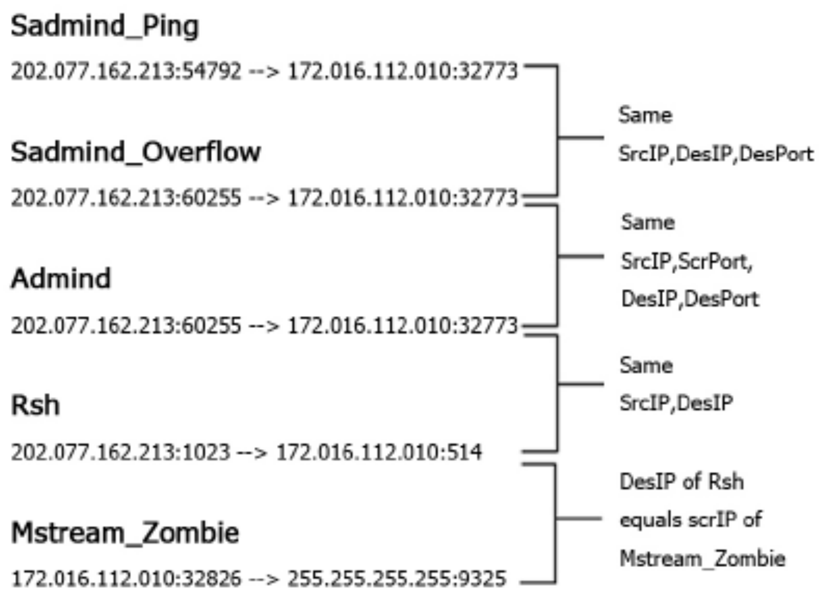
Rebuild the strategy of the DDoS attack

The offline alert correlation method extracted the causal relationships among different alert types and reconstructed the DDoS attack scenario.

Alert Type Pair	Correlation Probability	Relevant Features
<Sadmind Ping,Sadmind Overflow>	1.0	SrcIP,DesIP,DesPort
<Sadmind Ping, Admind>	1.0	SrcIP,DesIP,SrcPort,DesPort
<Admind, Rsh>	0.75	SrcIP,DesIP
<Rsh, Mstream Zombie>	0.79	DesIP of Rsh = ScrIP of Mstream Zombie

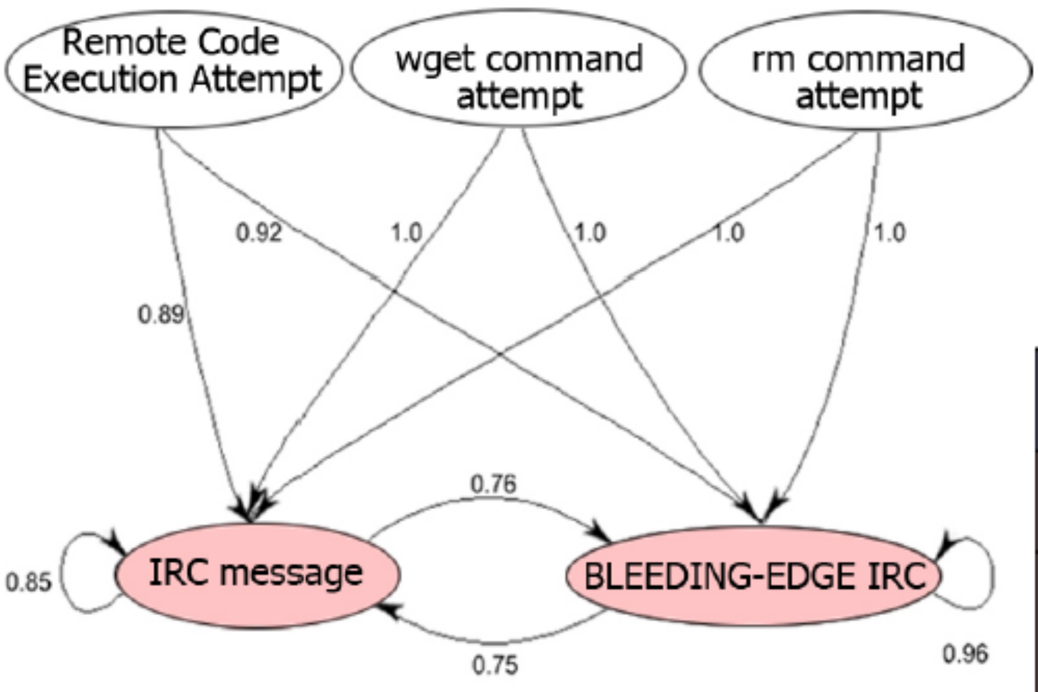
Accuracy	
TPC rate:	96.8%
FPC rate:	12.9%





Results on Honeynet dataset

The online alert correlation method's ability to adapt to the temporal changes of an alert's behavior:

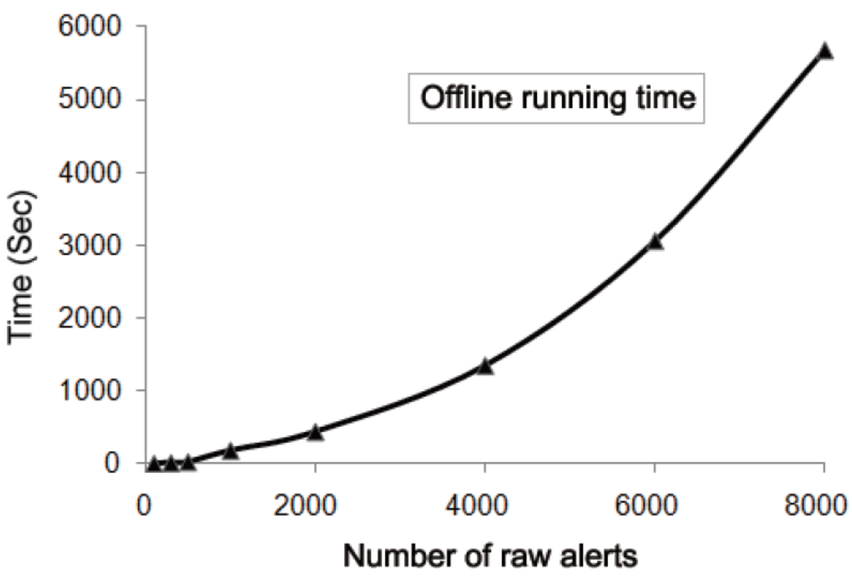


Offline correlation accuracy (data collected in Feb 25th)	
TPC rate:	96.5%
FPC rate:	15.9%

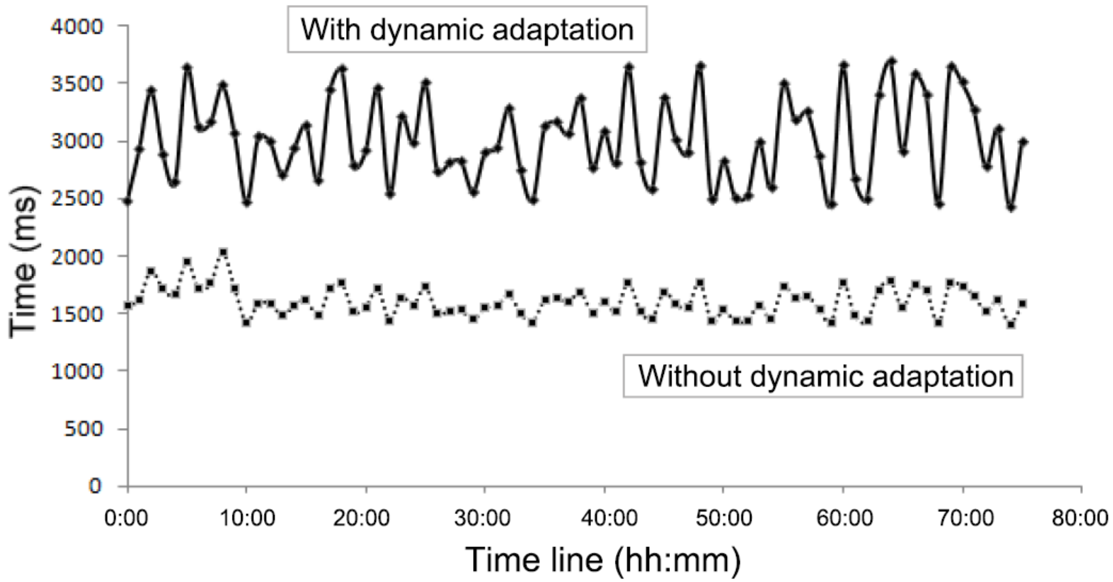
Online correlation accuracy (data collected in Feb 25th & Feb 26)	
Without Adaptive method	With Adaptive method
TPC rate: 93.2%	TPC rate: 96.1%
FPC rate: 15.9%	FPC rate: 14%

Performance test results

Offline Component



Online component



Conclusions

- This paper presents a new statistical based approach for correlating IDSs alerts and extracting attack scenarios:
  - Supports online alert correlation
  - Provides an unsupervised training method
  - Explicitly shows the reason of why two alerts are correlated

- Our approach successfully extracted the LLDOS1.0 attack scenario in Darpa date set with a high accuracy rate of 96.8%.

- Our approach can also adapt to the temporal changes in an alert's behavior.

- Our online correlation approach can reconstruct attack scenarios within a running time that roughly scales linearly with the size of raw alerts.

Future Work

- Introduce more configuration based features
- False positive alert detection
- Realtime intrusion prevention system
- Automatic adaptation of correlation threshold

Thank You!