An Online Adaptive Approach to Alert Correlation

Hanli Ren, Natalia Stakhanova, Ali A. Ghorbani

Information Security Centre of Excellence

MOTIVATION

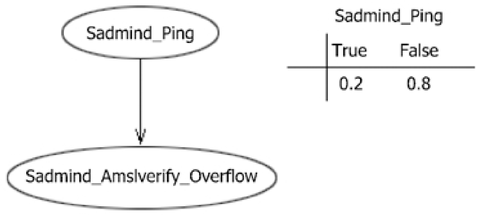
- IDSs usually generate a tremendous number of intrusion alerts
- Alert correlation techniques aiming to provide a succinct and high-level view of attacks gained a lot of interest.
- Majority of them address the alert correlation in the off-line setting

In this work, we focus on the online approach to alert correlation. Specifically, we propose a fully automated approach for online alert correlatio.

Bayesian network

- Describe causal or dependent relationships among variables
- Illustrate the strengths of these relationships

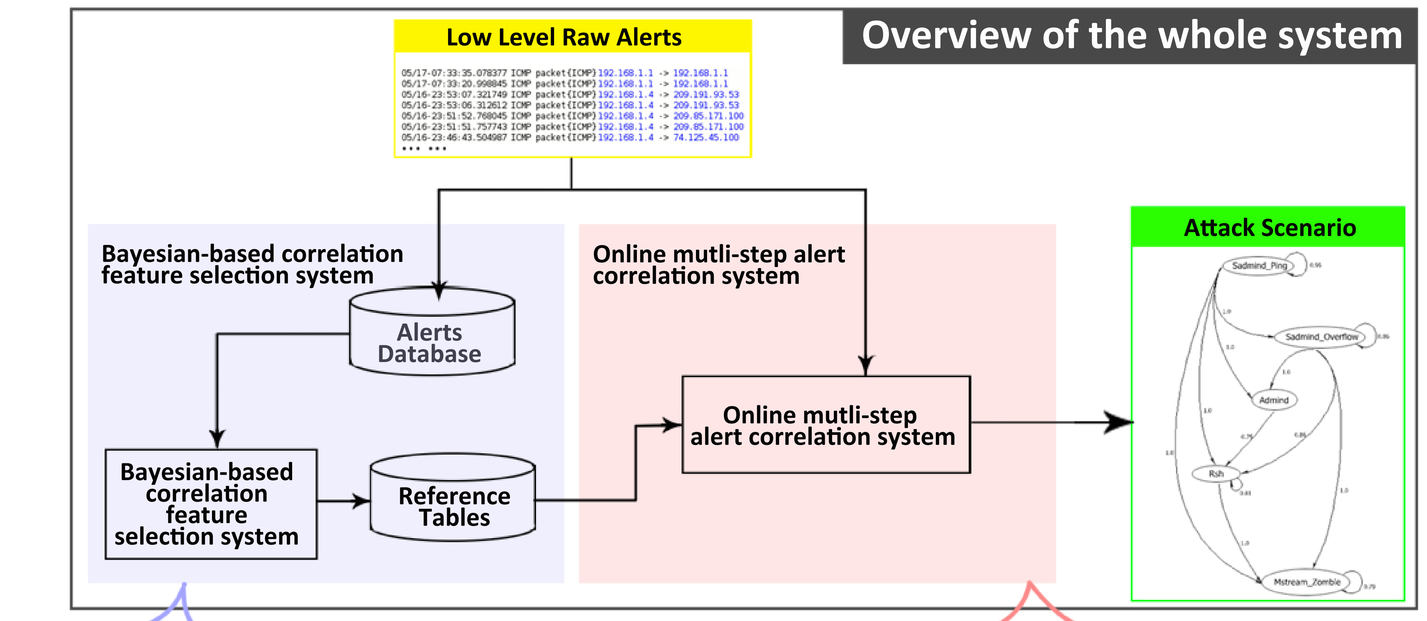
$$P(child = c|parent = p) = \frac{P(child = c \wedge parent = p)}{P(parent = p)}$$

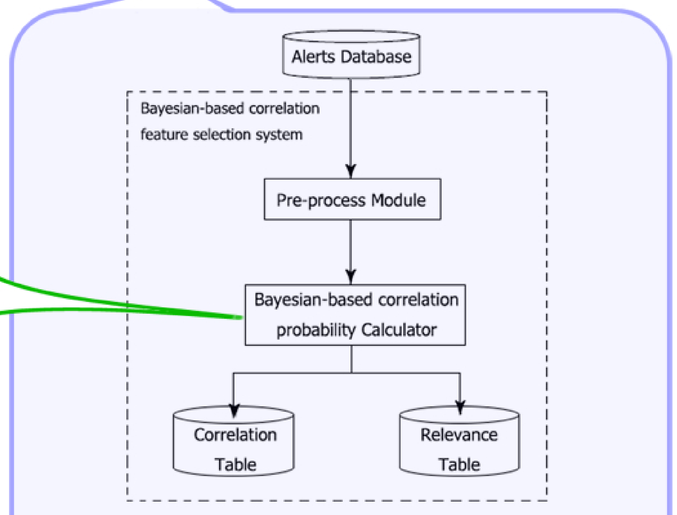


Sadmind_Ping	True	False
	0.2	0.8

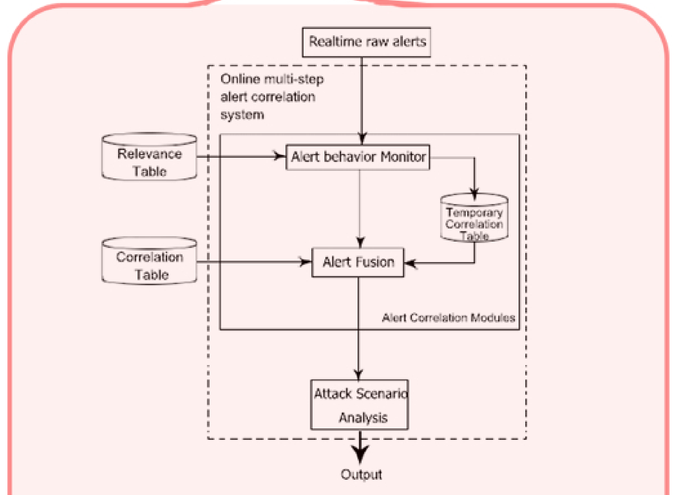
Sadmind_Ping	Sadmind_Amslverify_Overflow: True	False
True	0.9	0.1
False	0.01	0.99

FRAMEWORK





Overview of Offline Component

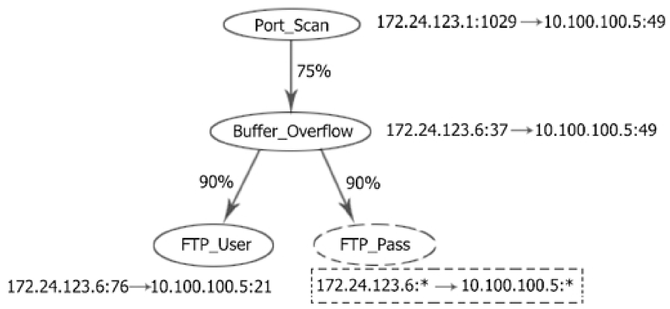


Overview of Online Component

RESULTS

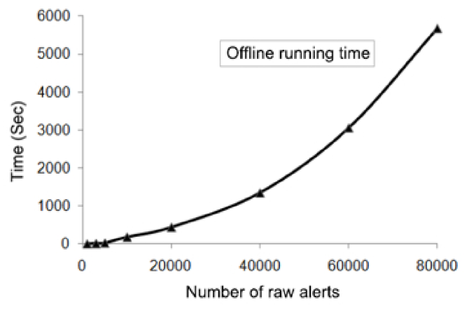
Attack scenario analysis and prediction

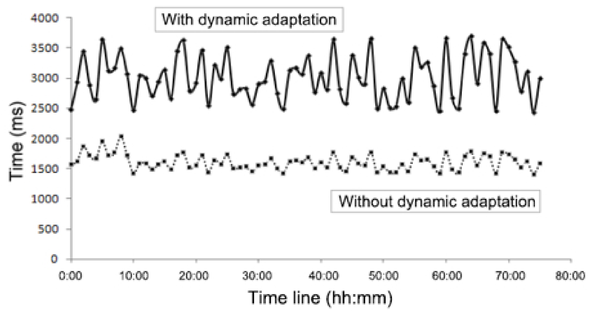
Alert Type Pair	Correlation Probability	Selected Features
<Port_Scan, Buffer_Overflow>	75%	DesIP,DesPort
<Buffer_Overflow, FTP_User>	90%	SrcIP,DesIP
<Buffer_Overflow. FTP_Pass>	90%	SrcIP,DesIP



An attack scenario is generated based on the pairs of causally related alerts.

Performance Test





CONTRIBUTIONS

The contributions of this work can be summarized as follows:

- ***A Bayesian correlation feature selection model*** that allows to automatically retrieve causal relationships and relevant features among alerts without expert or domain knowledge.
- ***An adaptive method for online attack scenario construction*** that allows a user to extract attack patterns in real time.
- ***An implementation*** of the proposed approach that allows a user to generate attack scenarios from a

Faculty of Computer Science
University of New Brunswick

UNB