



Network Security Situation Awareness Based on Spatio-temporal Correlation of Alarms

任泽华 3121154002

6.7.2022



CONTENTS

01

Introduction

- Background
- Research Motivation

02

Method Architecture

03

Demo System

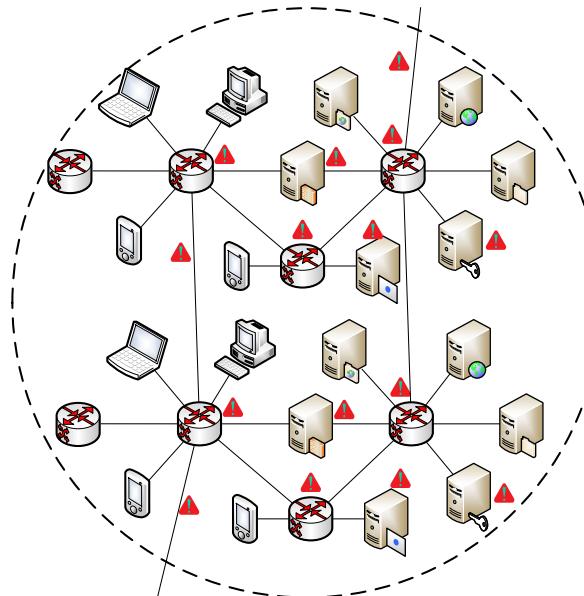
04

Conclusion

1. Introduction

1.1 Background

False Alarms in Intrusion Detection Systems (IDSs)



Massive alarm events

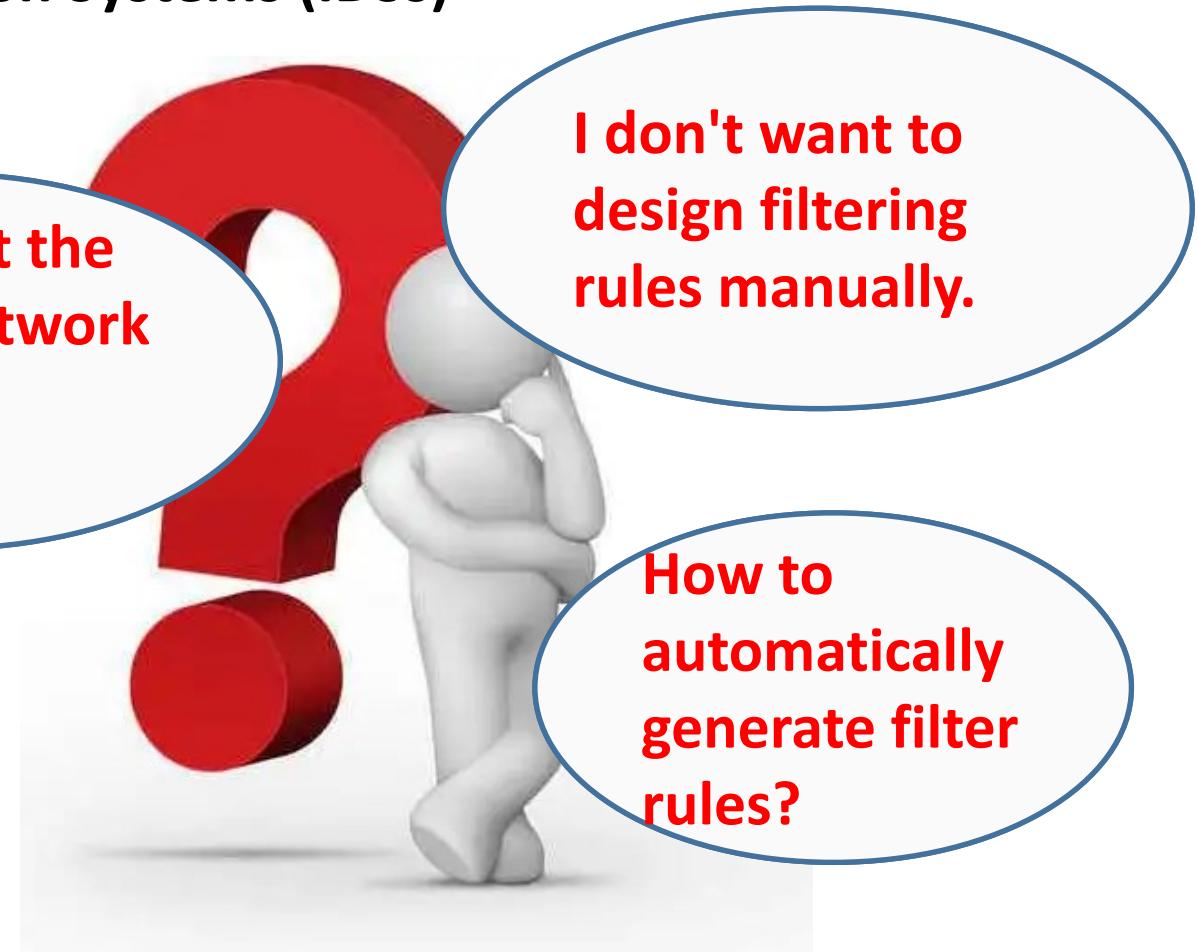


Network devices

How about the
current network
security
situation?

I don't want to
design filtering
rules manually.

How to
automatically
generate filter
rules?



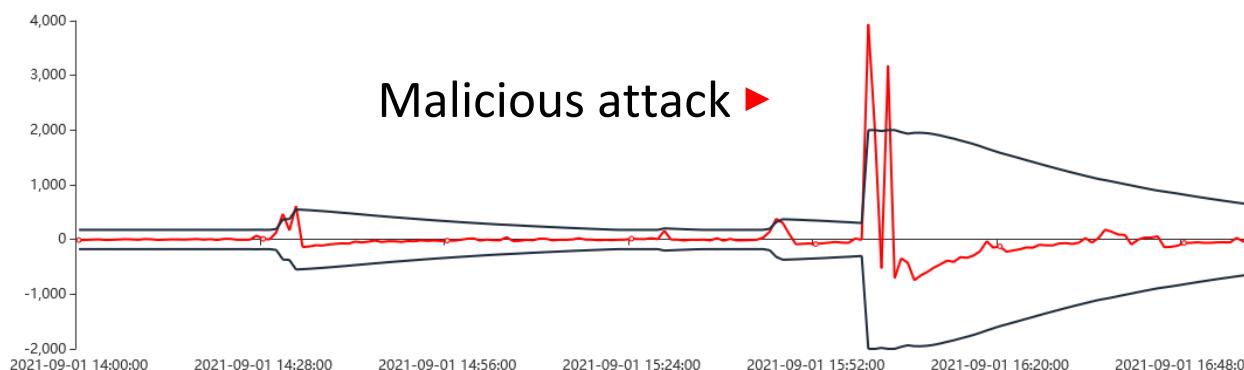
1. Introduction

1.2 Research Motivation

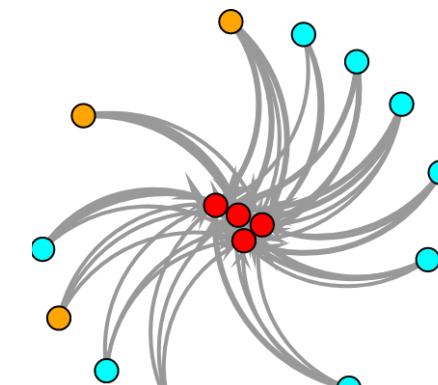
The spatio-temporal correlation of alarms.

Application scenarios:

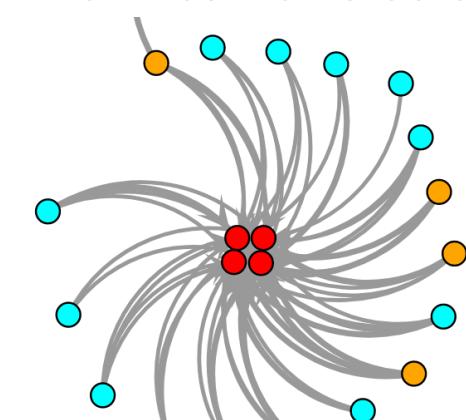
- Internal corporate network
- Industrial control network



2021-09-03 00:00:00



2021-09-16 18:00:00



● External device ● Internal user ● Partner company

Alarm type: MISC Attack Event type: Online conference

- Changes in statistical indicators over time reflect the occurrence of abnormal events.
- Different alarm graphs have same spatial structures: the same generate reasons.



CONTENTS

01 **Introduction**

02 **Method Architecture**

- Data Preprocessing
- Pattern Mining
- Similarity Analysis

03 **Demo System**

04 **Conclusion**

2. Method Architecture

2.1 Data Preprocessing

Original alarms data

id	receivetime	sip	sport	dip	dport	category	severity
457	2021-12-20 10:42:29	.211.18.180	18	.209.114.27	80	信息泄露	0
458	2021-12-20 10:43:33	.211.18.180	22	.209.114.27	80	信息泄露	0
459	2021-12-20 10:43:34	.209.32.159	06	.209.141.168	0	扫描器	1
460	2021-12-20 10:43:39	.211.18.180	28	.209.114.27	80	信息泄露	0
461	2021-12-20 10:43:39	.211.18.180	28	.209.114.27	80	信息泄露	0
462	2021-12-20 10:44:22	.211.18.180	31	.209.114.27	80	信息泄露	0
463	2021-12-20 10:45:51	.211.18.180	45	.209.114.27	80	信息泄露	0
464	2021-12-20 10:45:52	.211.18.180	49	.209.114.27	80	信息泄露	0
465	2021-12-20 10:45:59	.211.18.180	57	.209.114.27	80	信息泄露	0
466	2021-12-20 10:46:07	.211.18.180	70	.209.114.27	80	信息泄露	0
467	2021-12-20 10:46:09	.211.18.180	75	.209.114.27	80	信息泄露	0
468	2021-12-20 10:46:17	.211.18.180	84	.209.114.27	80	信息泄露	0
469	2021-12-20 17:39:39	.211.85.16	14	.209.30.14	77	信息泄露	0
470	2021-12-20 17:40:02	.209.32.159	85	.209.141.168	0	扫描器	1
471	2021-12-20 17:40:54	.211.71.58	97	.209.26.200	9	信息泄露	0
472	2021-12-20 17:40:54	.211.71.58	96	.209.30.14	77	信息泄露	0
473	2021-12-20 17:41:01	.211.132.18	63	.209.30.14	77	信息泄露	0
474	2021-12-20 17:41:01	.211.132.18	64	.209.26.200	9	信息泄露	0
475	2021-12-20 17:41:02	.209.32.159	94	.209.141.168	0	扫描器	1
476	2021-12-20 17:41:48	.211.132.38	41	.209.26.200	9	信息泄露	0

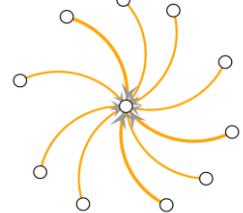


Node: IP address

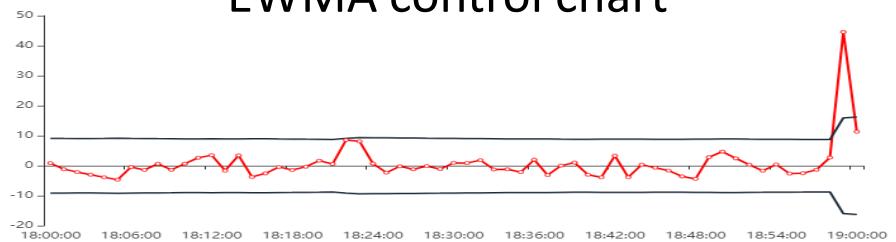


Edge: alarm event

Alarm graph



EWMA control chart

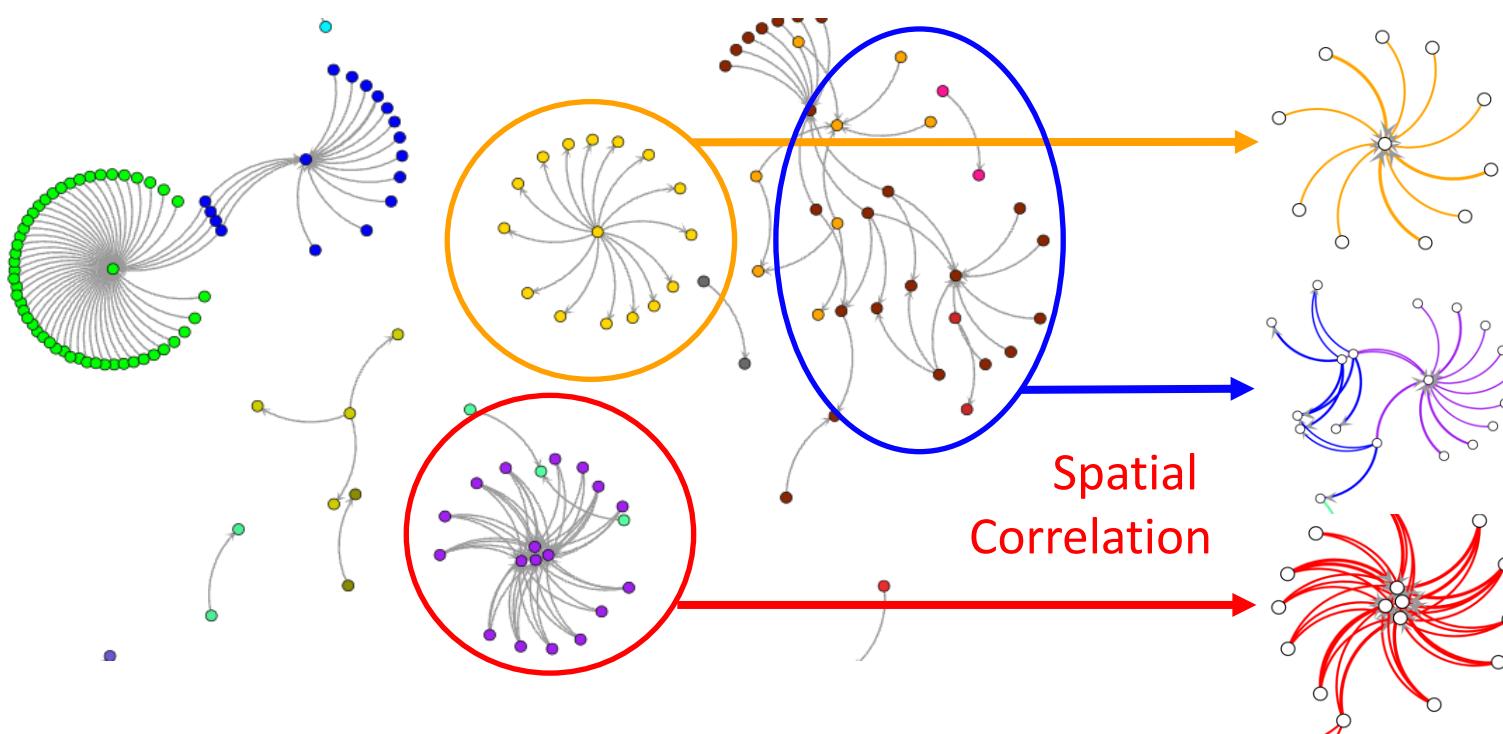


- Using Exponential Weighted Moving Average method to find abnormal behaviors.
- Dynamically set time window according to the current security situation.

2. Method Architecture

2.2 Pattern Mining

- Find alarm groups by community discovery algorithm.
- Classify alarm clusters according to topology characteristics.



Single-center Topology

Complex Topology

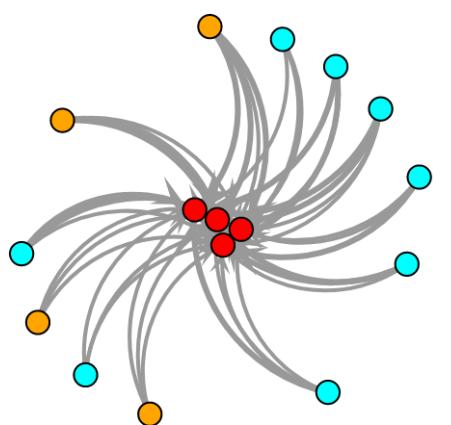
Multi-center Topology

2. Method Architecture

2.3 Similarity Analysis

Event Model: Online conference

2021-09-03 00:00:00



● External device ● Internal user ● Partner company

Type: MISC Attack 100%

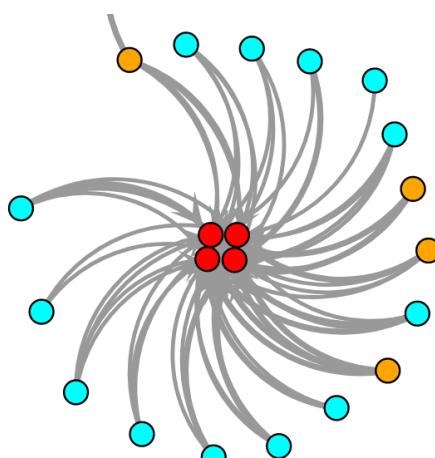
Center: External device

Around: Part-comp 33%

Subgraph motifs:



2021-09-16 18:00:00



● External device ● Internal user ● Partner company

Type: MISC Attack 100%

Center: External device

Around: Part-comp 25%

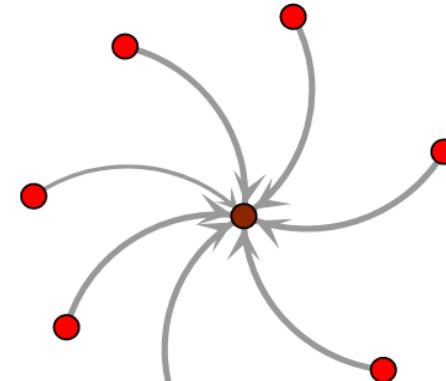
Subgraph motifs:



Spatio-temporal Correlation

Event Model: Conventional attack

2021-09-04 14:00:00



● External device

Type: Info leakage 100%

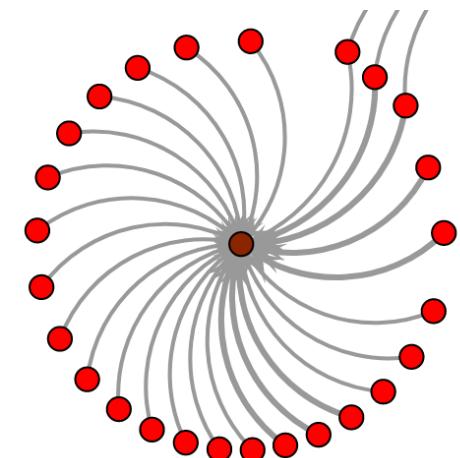
Center: Critical server

Around: External 100%

Subgraph motifs:



2021-10-02 10:00:00



● Critical server

Type: Info leakage 99%

Center: Critical server

Around: External 100%

Subgraph motifs:





CONTENTS

01 **Introduction**

02 **Method Architecture**

03 **Demo System**

- System Overview
- Core Function

04 **Conclusion**

3. Demo System

3.1 System Overview

The screenshot shows the 'Power Grid Situation Awareness System' interface. On the left, a sidebar includes 'Real-time alarm', 'Alarm Pattern Mining', 'EWMA Control Charts', 'Historical alarm', and 'Outer link' buttons. The main area features a large, dense network graph with nodes of various colors (red, green, blue, yellow) and many connecting lines. To the right of the graph is a 'Edge details' panel with the following data:

- Current clusters number: 38
- Source IP: 127.23.186.60
- Destination IP: 195.186.76.139
- Repeat Times: 1

Below this is an 'Alarm Details' table:

Num	Time	Manufacturer	Type
0	2021-09-05 09:44:33	device1	选项应用 软件

- Security risk assessment.
- Alarm handling.

- Alarm graph visualization.
- Check alarm details.

The screenshot shows the same 'Power Grid Situation Awareness System' interface. The network graph now highlights a specific pattern of nodes and connections with a red circle. To the right is an 'Alarm details' panel with the following information:

- Current clusters number: 37

Below this is a list of instructions:

1. This area is used to display alarm details.
2. Click the node or edge to show the details of the corresponding IP or single alarm.
3. Double-click the node or edge to display the related content of the corresponding pattern.
4. Click 'Clear' on the upper left corner can return to this page.
7. Click 'Mark' on the upper right corner of the group page can mark the pattern.

3. Demo System

3.2 Core Function

The screenshot displays the 'Power Grid Situation Awareness System' interface with three main functional areas:

- 1. Detecting abnormal events**: Located on the left, this section includes a search bar for 'Please enter the IP' and 'Search', and two line charts: 'Number of alarm devices' and 'Number of alarms'. The 'Number of alarm devices' chart shows a fluctuating line with red markers for error, upper, and lower thresholds. The 'Number of alarms' chart shows a similar fluctuating line with the same threshold markers. A red arrow points from this section to a network graph on the right.
- 2. Locating event on graphs**: This is the network graph on the right, showing nodes (dots) and edges (lines) representing the relationships between alarm devices. A red arrow points from the 'Number of alarms' chart to this graph.
- 3. Matching similar events**: Located on the right, this section is titled 'Alarm Pattern details' and shows 'Original pattern' and 'Similar pattern' network graphs. It includes details such as 'Number: 1', 'Alarm: 76', 'Nodes: 15', 'Edges: 41', and 'Origin: Multi-center'. A red arrow points from the network graph to this section.

Demo video at <https://bit.ly/NSSA-ST>



CONTENTS

01 **Introduction**

02 **Method Architecture**

03 **Demo System**

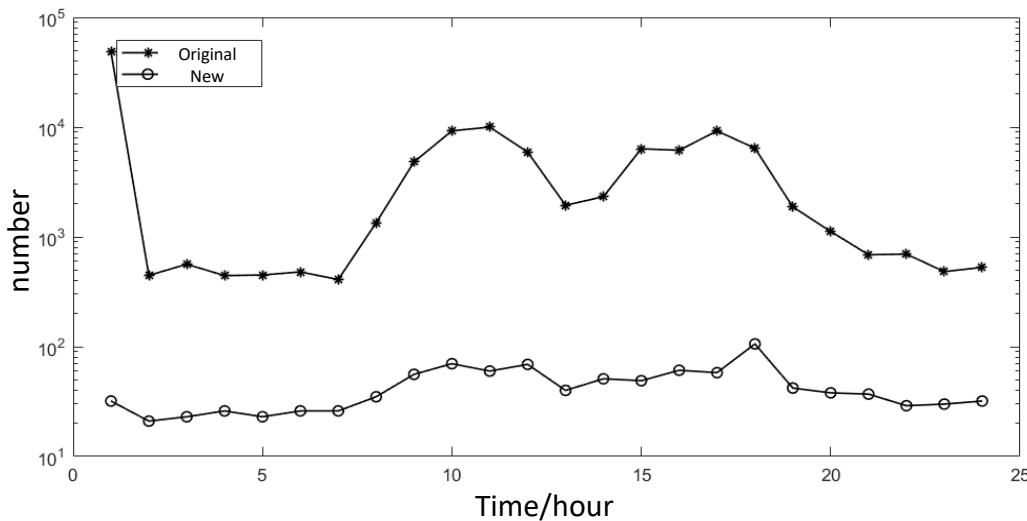
04 **Conclusion**

➤ Conclusion

4. Conclusion

4.0 Conclusion

- We developed a network security situation awareness (NSSA) system based on the spatio-temporal correlation of alarms.
- Our system can detect high risk patterns semi-automatically and deal low-risk alarms automatically based on historical operations.
- Compared with the old system, our system has better performance and richer functions.



Performance	Original system	Our system
Processing time	More than 10"	Less than 1"
Data scale	10 ³ -10 ⁵	10 ¹ -10 ²
Accuracy	70%	95%
Cross-platform	no	yes
Similar matching	no	yes



Thank you!
Q&A

Zehua Ren
renzehua@stu.xjtu.edu.cn

6.7.2022