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

任泽华 3121154002

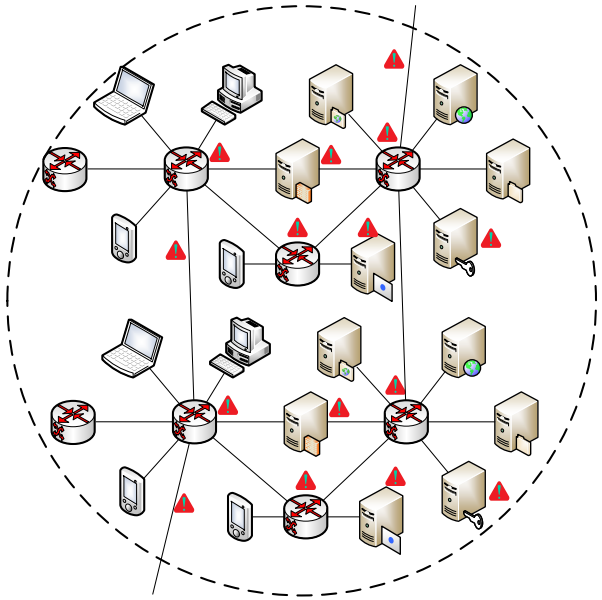
6.7.2022

CONTENTS

1. Introduction

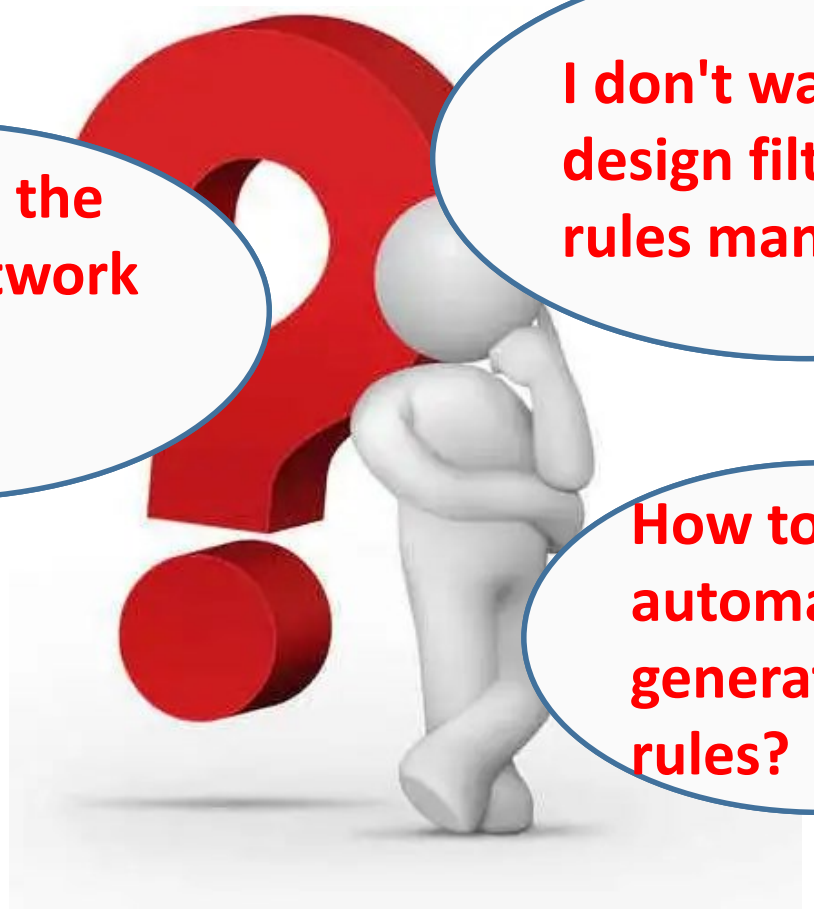
1.1 Background

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?

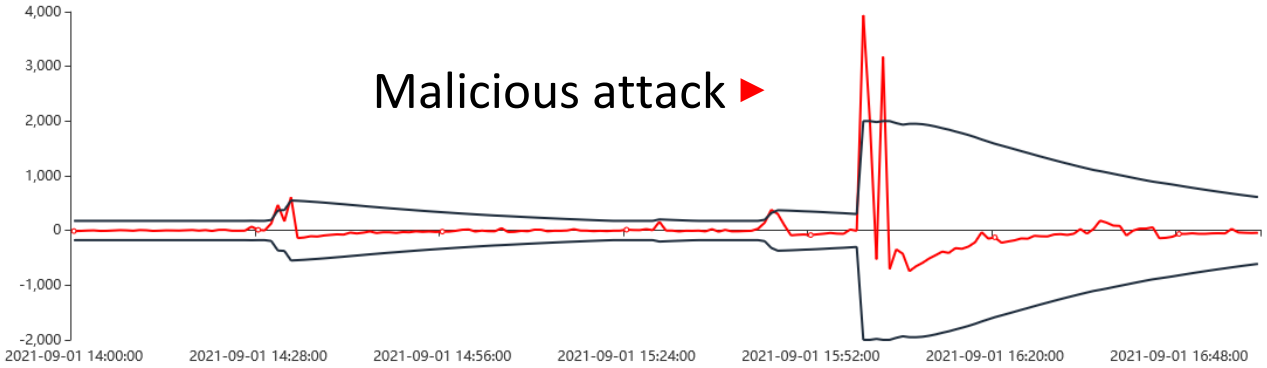
1. Introduction

1.2 Research Motivation

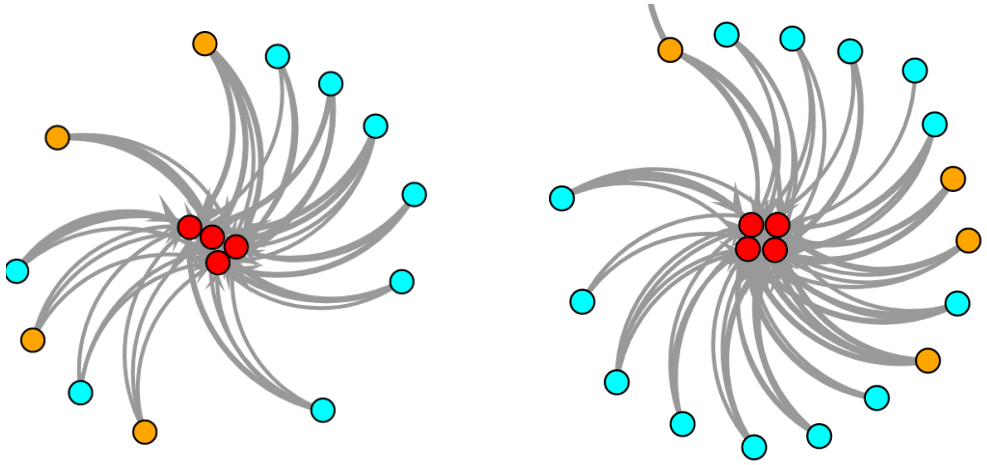
The spatio-temporal correlation of alarms.

☑ 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

2. Method Architecture

2.1 Data Preprocessing

Original alarms data

id	receivetime	sip	sport	dip	dport	category	severity
457	2021-12-20 10: :29	.211.18.180	18	.209.114.27	80	信息泄露	0
458	2021-12-20 10: :33	.211.18.180	22	.209.114.27	80	信息泄露	0
459	2021-12-20 10: :34	.209.32.159	06	.209.141.168	0	扫描器	1
460	2021-12-20 10: :39	.211.18.180	28	.209.114.27	80	信息泄露	0
461	2021-12-20 10: :39	.211.18.180	28	.209.114.27	80	信息泄露	0
462	2021-12-20 10: :42	.211.18.180	31	.209.114.27	80	信息泄露	0
463	2021-12-20 10: :51	.211.18.180	45	.209.114.27	80	信息泄露	0
464	2021-12-20 10: :52	.211.18.180	49	.209.114.27	80	信息泄露	0
465	2021-12-20 10: :59	.211.18.180	57	.209.114.27	80	信息泄露	0
466	2021-12-20 10: :07	.211.18.180	70	.209.114.27	80	信息泄露	0
467	2021-12-20 10: :09	.211.18.180	75	.209.114.27	80	信息泄露	0
468	2021-12-20 10: :17	.211.18.180	84	.209.114.27	80	信息泄露	0
469	2021-12-20 17: :39	.211.85.16	14	.209.30.14	77	信息泄露	0
470	2021-12-20 17: :02	.209.32.159	85	.209.141.168	0	扫描器	1
471	2021-12-20 17: :54	.211.71.58	97	.209.26.200	9	信息泄露	0
472	2021-12-20 17: :54	.211.71.58	96	.209.30.14	77	信息泄露	0
473	2021-12-20 17: :01	.211.132.187	63	.209.30.14	77	信息泄露	0
474	2021-12-20 17: :01	.211.132.187	64	.209.26.200	9	信息泄露	0
475	2021-12-20 17: :02	.209.32.159	94	.209.141.168	0	扫描器	1
476	2021-12-20 17: :48	.211.132.38	41	.209.26.200	9	信息泄露	0

Time window

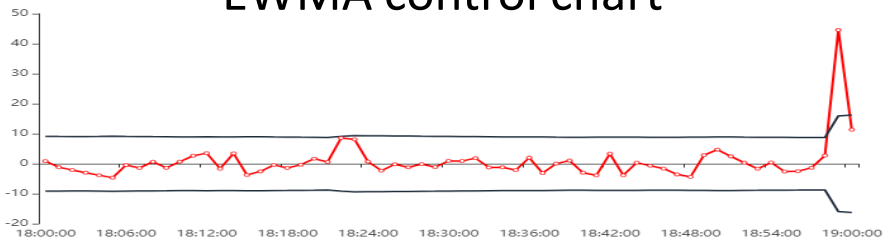
Node: IP address

Edge: alarm event

Alarm graph

Temporal Correlation

EWMA control chart

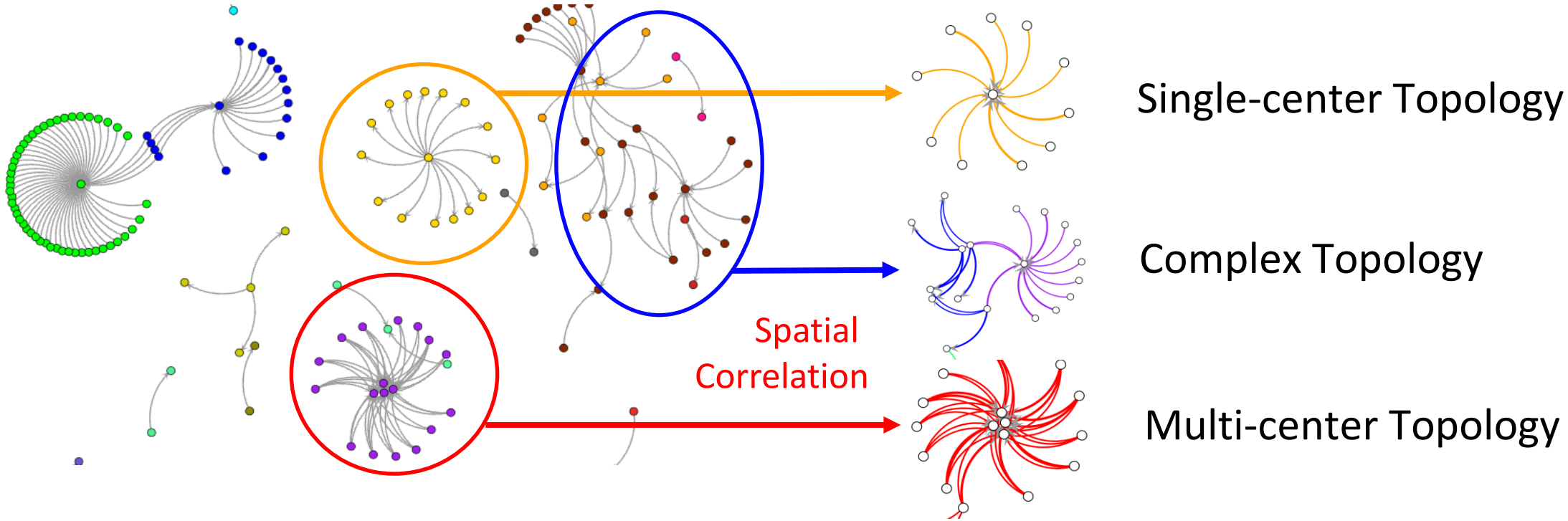


- **Using Exponential Weighted Moving Average method to find abnormal behaviors.**
- **Dynamically set time window according to the current security situation.**

2. Method Architecture

2.2 Pattern Mining

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



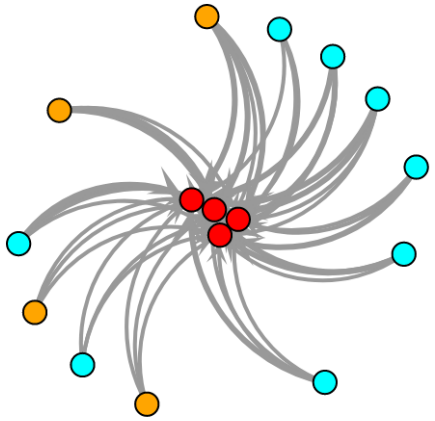
2. Method Architecture

2.3 Similarity Analysis

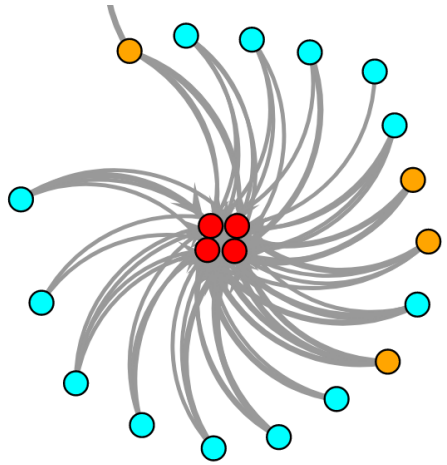
Spatio-temporal Correlation

Event Model: **Online conference**

2021-09-03 00:00:00



2021-09-16 18:00:00



External device Internal user Partner company

Type: MISC Attack 100%

Center: External device

Around: Part-comp 33%

Subgraph motifs:

 6.10%  91.35%

Type: MISC Attack 100%

Center: External device

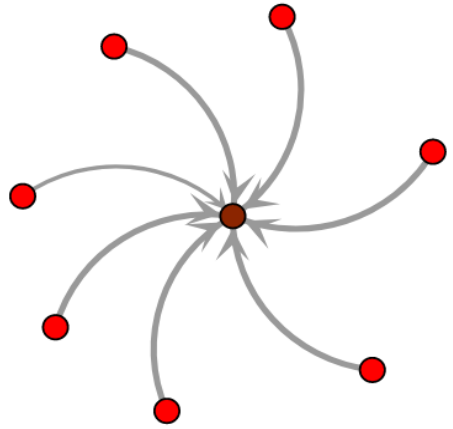
Around: Part-comp 25%

Subgraph motifs:

 5.88%  94.12%

Event Model: **Conventional attack**

2021-09-04 14:00:00



External device

Type: Info leakage 100%

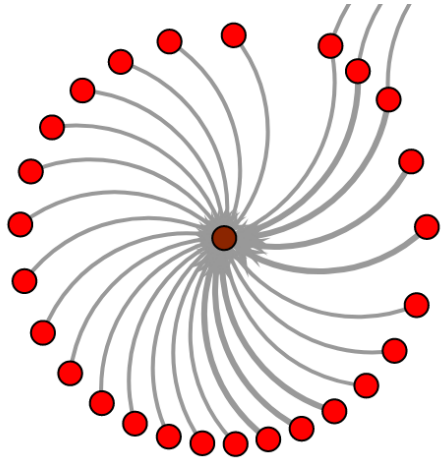
Center: Critical server

Around: External 100%

Subgraph motifs:

 0%  100%

2021-10-02 10:00:00



Critical server

Type: Info leakage 99%

Center: Critical server

Around: External 100%

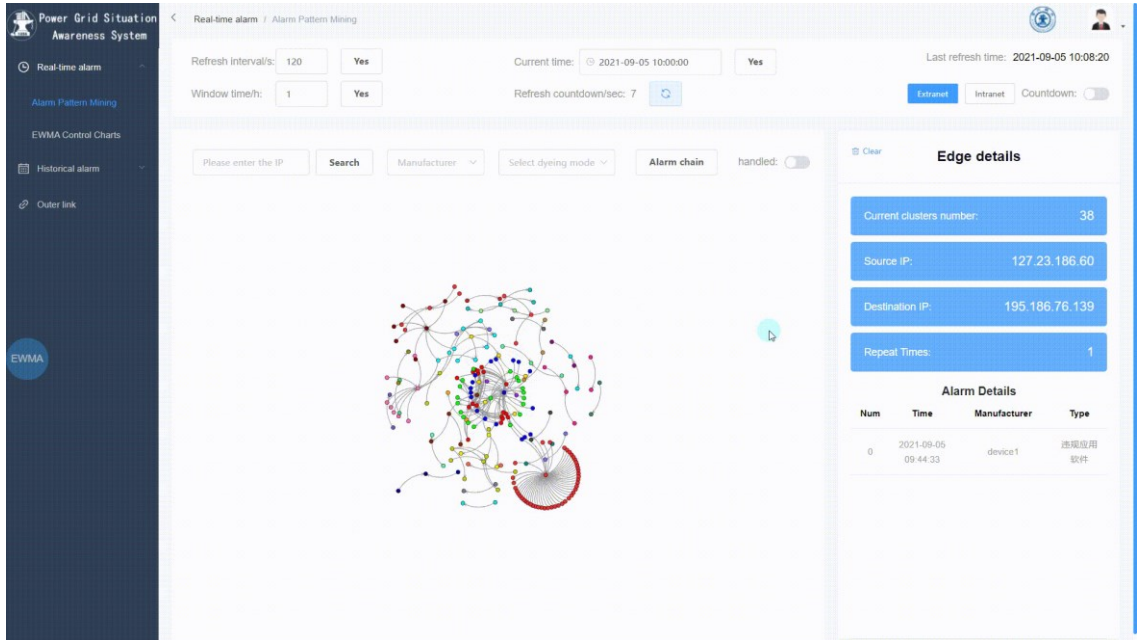
Subgraph motifs:

 0%  100%

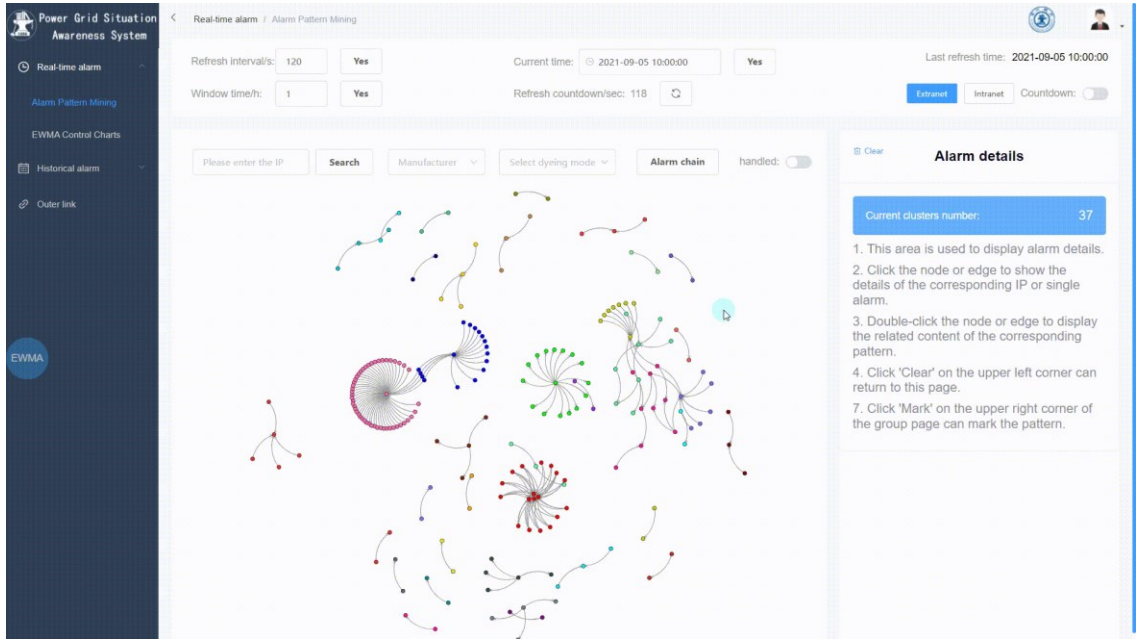
CONTENTS

3. Demo System

3.1 System Overview



- Alarm graph visualization.
- Check alarm details.

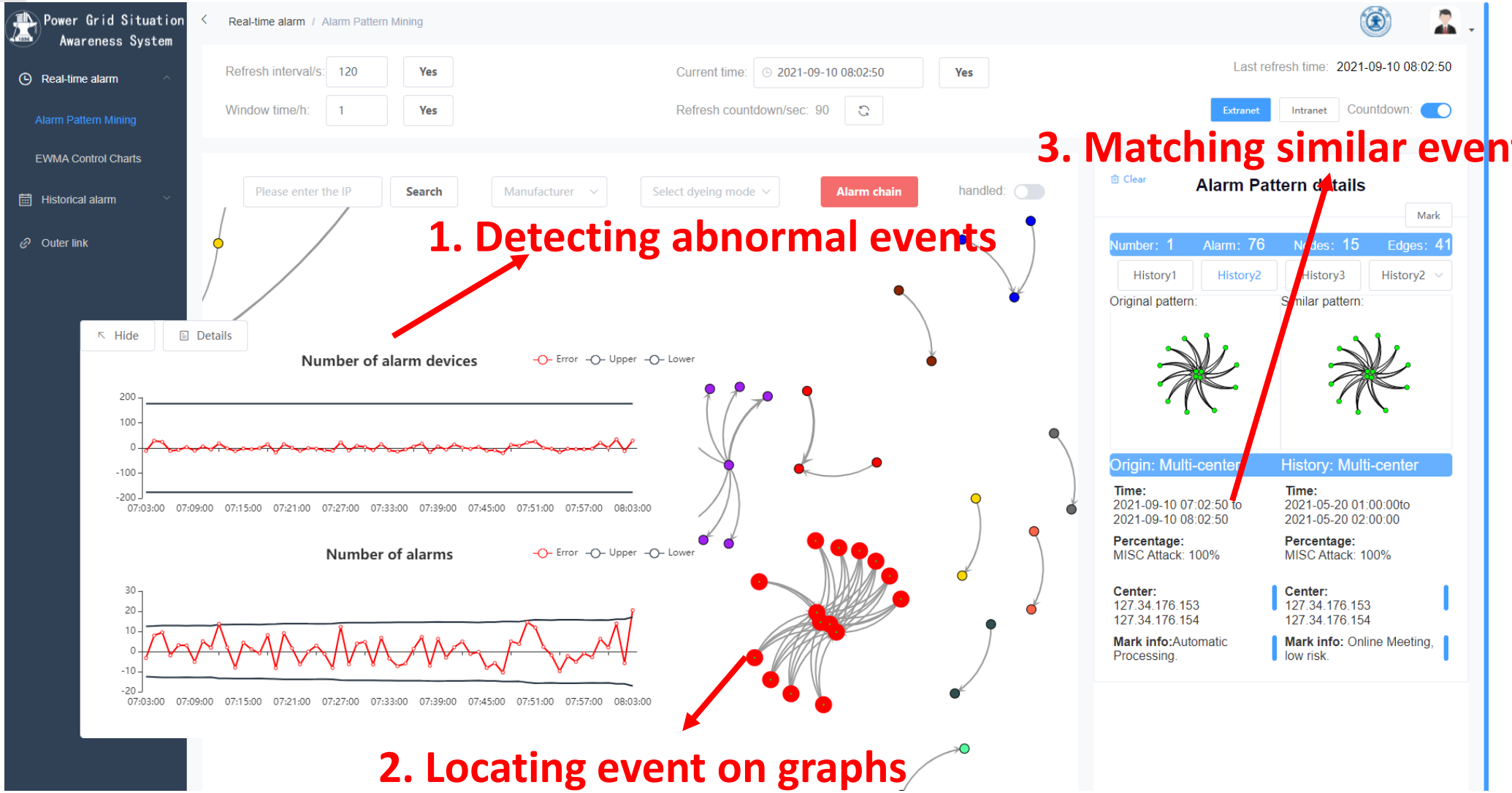


- Security risk assessment.
- Alarm handling.

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

3. Demo System

3.2 Core Function



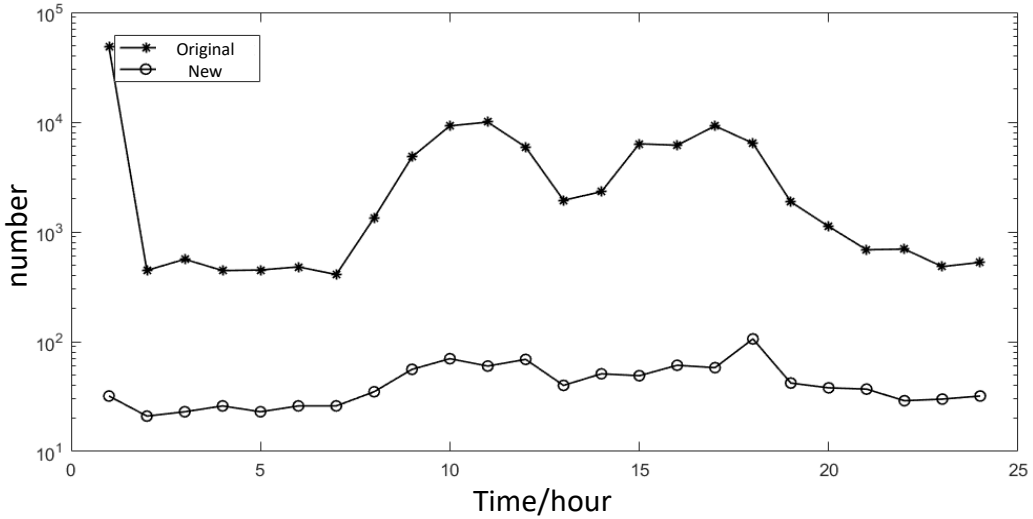
Demo video at https://bit.ly/NSSA-ST

CONTENTS

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