Discovering causal relationships between events in device logs

QUT SEF VRES 2021 Showcase

Supervisors: Dr Zahra Jadidi, Professor Daniel Quevedo, Dr Tanvir Ul Huque

By Joshua Hagemann

I. Introduction

Industrial Control Systems (ICSs) are increasingly the target of multi-phase, sophisticated cyber-attacks called Advanced Persistent Threats (APTs). The attack's true purpose is often obfuscated making mounting a defence difficult. ICS APT attacks use multiple steps to reach their target devices. Causal analysis of anomalies in device logs can help to detect these attacks in early phases before the final stage of the attacks can be executed against ICS endpoints. Developing causal relationship graphs for events prior to, during, and after an attack gives insight the operations of the system and can be used to create a plan-of-action to stop the APT from achieving its final goals.

II. Aim

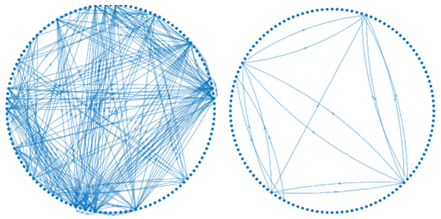
Analyse the effectiveness of a causal algorithm in identifying causal relationships of ICS APT attacks

III. Causal algorithm

- A causal relationship is defined by: "*cause is that which put, the effect follows; and removed, the effect is removed*"
- The algorithm used detects causality between individual intrinsic mode functions (IMFs) within a time series [4].
- The IMFs correspond to different frequencies and residue which make up the components of the time series [5].
- If the attack IMF is removed, then the causal response from that attack will also be removed.

TABLE I
SCENARIOS FOR EACH DATASET

Scenario	Description of Scenario
	SWaT Dataset
1	Attack on sensor FIT401: Spoof value from 0.8 to 0.5
2	Attack on sensor LIT301: Spoof value from 835 to 1024
3	Attack on sensor P601: Switch from OFF to ON
4	Multi-point attack on sensor MV201 and P101: Switch from CLOSE to OPEN (MV201) and OFF to ON (P101)
5	Attack on sensor MV501: Switch from OPEN to CLOSE
6	Attack on sensor P301: Switch from ON to OFF
normal	Normal operational conditions for all sensors
	Power System Dataset
41	No Event: Normal Operation load changes
19	Remote Tripping Command Injection: Command Injection to R1 and R2
15	Remote Tripping Command Injection: Command Injection to R1



221 Causal relationships 14 Causal relationships

Fig. 1. Causal relationships discovered for Scenario 41, dataset no. 1 which have a threshold score greater than 0.4 (left) and greater than 0.75 (right)

IV. Datasets used

A. Power System Attack Datasets

- There were 128 unique devices used in collecting data for the operation of the system [6].
- The data recorded is primarily analogue values.

B. Secure Water Treatment (SWaT) Dataset

- There were 77 unique devices used in collecting data for the operation of the system [7].
- The data recorded is a mix of analogue and digital values.

V. Accuracy of causal relationships

Each dataset was sampled at 20%, and the causal relationships recalculated. The accuracy when compared to the original dataset is defined as:

$$(no.\ similar) / (no.\ similar + no.\ different)$$

The accuracy was calculated over a range of thresholds to identify which causal threshold gave the most accurate data.

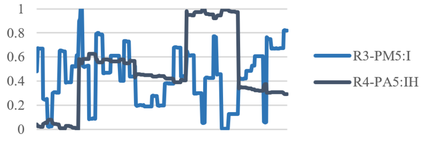


Fig. 2. Scenario 41 dataset no. 2 normalized showing device log R3-PM5 and R4-PA5:IH. The causal relationship score of these device logs is 0.3005

VI. Impact of threshold on causal relationships

The absolute causality score calculated for each device log ranges from 0 to 1. The higher the threshold score, the greater the correlation of a time series is to another, and the more likely it can be recognised by human pattern recognition.

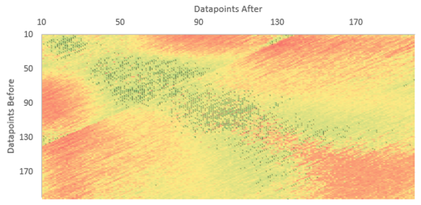


Fig. 4. Scenario 1 showing absolute causal score between FIT401 and UV401 where a higher score is green, and a lower score is red.

TABLE 2
20 PERCENT ACCURACY TEST FOR CASUAL RELATIONSHIPS

Scenario	No. data points	Highest accuracy	Threshold value
	SWaT Dataset		
1	105	0.037037	0.402
2	273	0	0
3	232	0.05	0.445
4	451	0.057377	0.302
5	121	0	0
6	803	0	0
normal	200	0.16667	0.549
	Power System Dataset		
41			
data 1	173	0.3871	0.51
data 2	322	0.4	0.624
data 3	354	1	0.752
19			
data 1	167	0.34545	0.568
data 2	142	0.35172	0.53
data 3	65	1	0.729
15			
data 1	132	1	0.737
data 2	137	0.61635	0.65
data 3	19	n/a	n/a

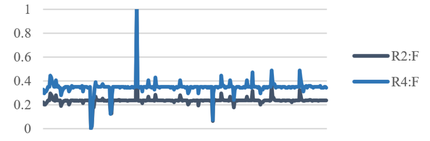


Fig. 3. Scenario 41 dataset no. 2 normalized showing device log R2:F and R4:F. The causal relationship score of these device logs is 0.5251

VII. Prior data vs. ground truth

The causal algorithm will not find a relationship when the timeseries is constant. To correctly identify the causal relationship, data prior to or succeeding the attack scenario is required.

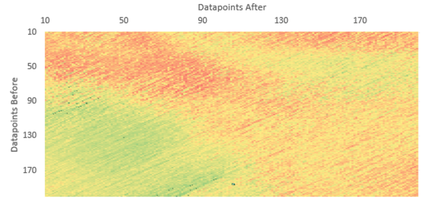


Fig. 5. Scenario 3 showing absolute causal score between P601 and LSH601 where a higher score is green, and a lower score is red.

TABLE 3
OPTIMISING TIME SERIES DATA

Scenario	Correct ground truth
	SWaT Dataset
1	
Data prior	No
Datapoints prior and during (unoptimized)	Yes
Datapoints prior and during (optimized)	Yes
Data during only	No
4	
Data prior	No
Datapoints prior and during (unoptimized)	No
Datapoints prior and during (optimized)	Yes
Data during only	No
Power System Dataset	
19	
Data prior	No
Data prior and during (unoptimized)	Yes
Data prior and during (optimized)	Yes
Data during only	Yes
15	
Data prior	No
Data prior and during (unoptimized)	Yes
Data prior and during (optimized)	Yes
Data during only	Yes

VIII. Conclusion

Determining the required threshold value is essential to extracting meaningful causal relationships from events in device logs.

- A low threshold increases the number of false positive causal relationships.
- A high threshold may eliminate unoptimized attack data or reveal no new information about the time series.

The threshold value and the no. data points needed to optimize causal results is dependent on the dataset and attack types.

- Digital devices in ICSs require optimization of the attack pattern in order to be correctly identified.
- Analogue devices in ICSs where attacks occur over an extended period do not require optimization.

Future work may include investigating the noise level of different ICSs to better calculate a threshold value which minimizes the number of false positive causal relationships.

IX. References

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research,* vol. 1, p. 80, 2011.

[2] M. Khosravi and B. T. Ladani, "Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection," *IEEE Access,* vol. 8, pp. 162642-162656, 2020.

[3] J. Vávra and M. Hromada, "An evaluation of cyber threats to industrial control systems," in *International Conference on Military Technologies (ICMT) 2015*, 2015, pp. 1-5.

[4] Yang, A.C., Peng, CK. & Huang, N.E., "Causal decomposition in the mutual causation system.," *Nat Commun,* pp. 1-9, 2018.

[5] Bi-Ling Huang and Yuan Yao, Batch-to-batch Steady State Identification via Online Ensemble Empirical Mode Decomposition and Statistical Test, vol. 33, J. J. K. a. P. S. V. a. P. Y. Liew, Ed., 2014, pp. 787-792.

[6] Mississippi State University Critical Infrastructure Protection Center, "Industrial Control System Cyber Attack Data Set," Apr 2014. [Online]. Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.

[7] Goh, Jonathan & Adepu, Sridhar & Junejo, Khurum & Mathur, Aditya, "A Dataset to Support Research in the Design of Secure Water Treatment Systems," 2016.