Real-Time Machine Learning for Power Grid SCADA Alarm Event Detection Decision Support

Chen Liu[1], Geordie Dalzell[1], Elena Kranz[2], Xinghuo Yu[1], Adrian Kelly[3], Mahathir Almashor[4]

[1]School of Engineering, RMIT University, Australia.

[2]Technical University of Berlin, Germany.

[3]Electric Power Research Institute (EPRI), Ireland.

[4]Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia.

RMIT UNIVERSITY

Summary

- Introduction
- Methodology
  - Alarm event detection model training
  - Alarm event decision support
- Empirical Study
- Conclusion

RMIT UNIVERSITY

Introduction

- Intelligent analysis and regulation
  - Enhancing power grid efficiency and reliability.

- Supervisory Control And Data Acquisition (SCADA) and Energy Management System (EMS)
  - Two major systems for power fault detection.

- Detect anomalous behaviors in SCADA systems is the key challenge.

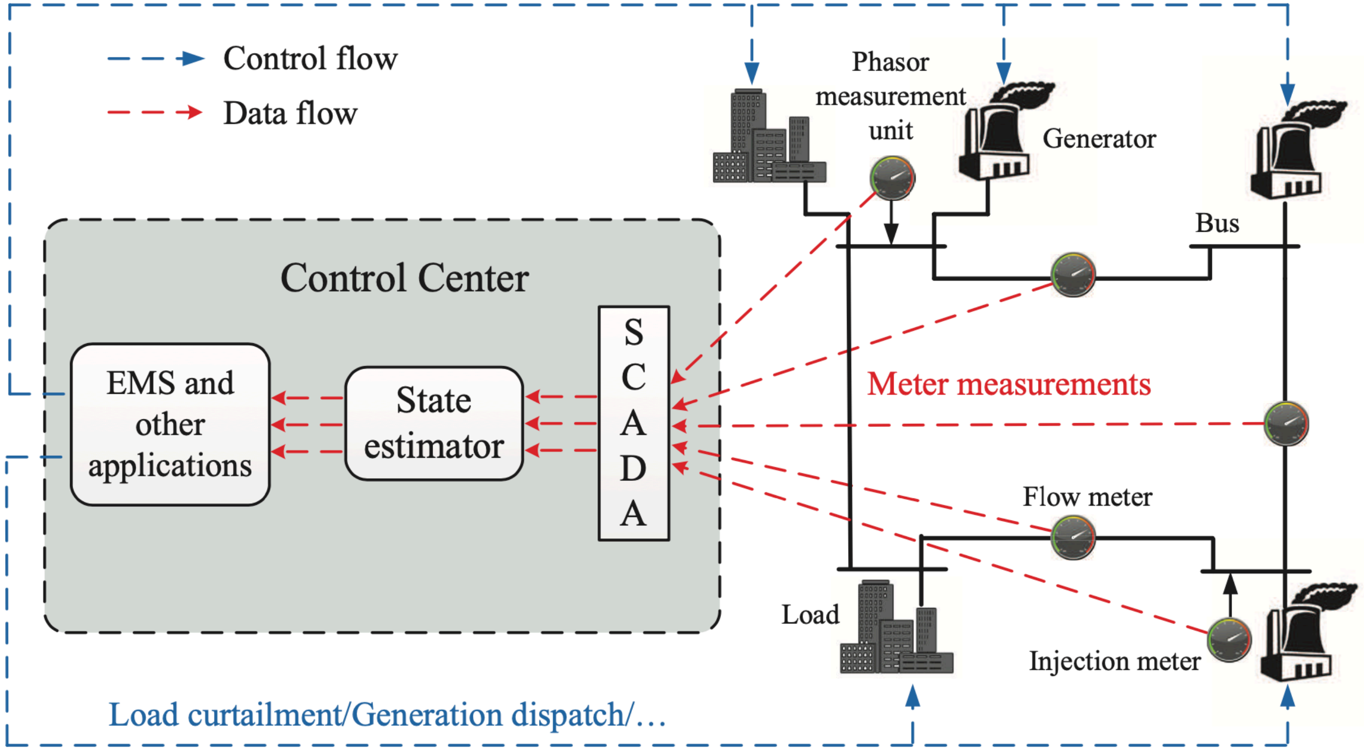


Fig. 1 The operation of the SCADA/EMS system in power grid [1]

Introduction

- Intelligent alarm processing in power systems
  - Rule-based systems for alarm classification. [2,3]
  - Expert systems: make decision support faster. [4,5,6]
  - Mixed integer linear programming for false alarms detection. [7,8]
- **Motivation:**
  - Current research on real-time power system SCADA setups remains limited.
  - A critical need exists to develop solutions for the early detection and mitigation of potential stability events.
  - Previous work focuses primarily on peak alarm periods, leaving operators with insufficient time to respond to incidents and learn from past experiences.

Introduction

- **Contributions:**
  - Novel Deep Neural Network (DNN) Framework
    - **Offline training** using historical alarm data for robust generalization.
    - **Accurate detection** of critical SCADA alarm events, especially during peak periods when operators require enhanced decision-making support.
  - Online Decision Support Framework
    - Combines a **pre-trained DNN** with a **large language model (LLM)**.
    - **Real-time alarm detection** and prioritization of event information based on historical urgency and relevance.
    - Provides a **holistic view** for operators, supporting **quick and informed decision-making.**

Methodology

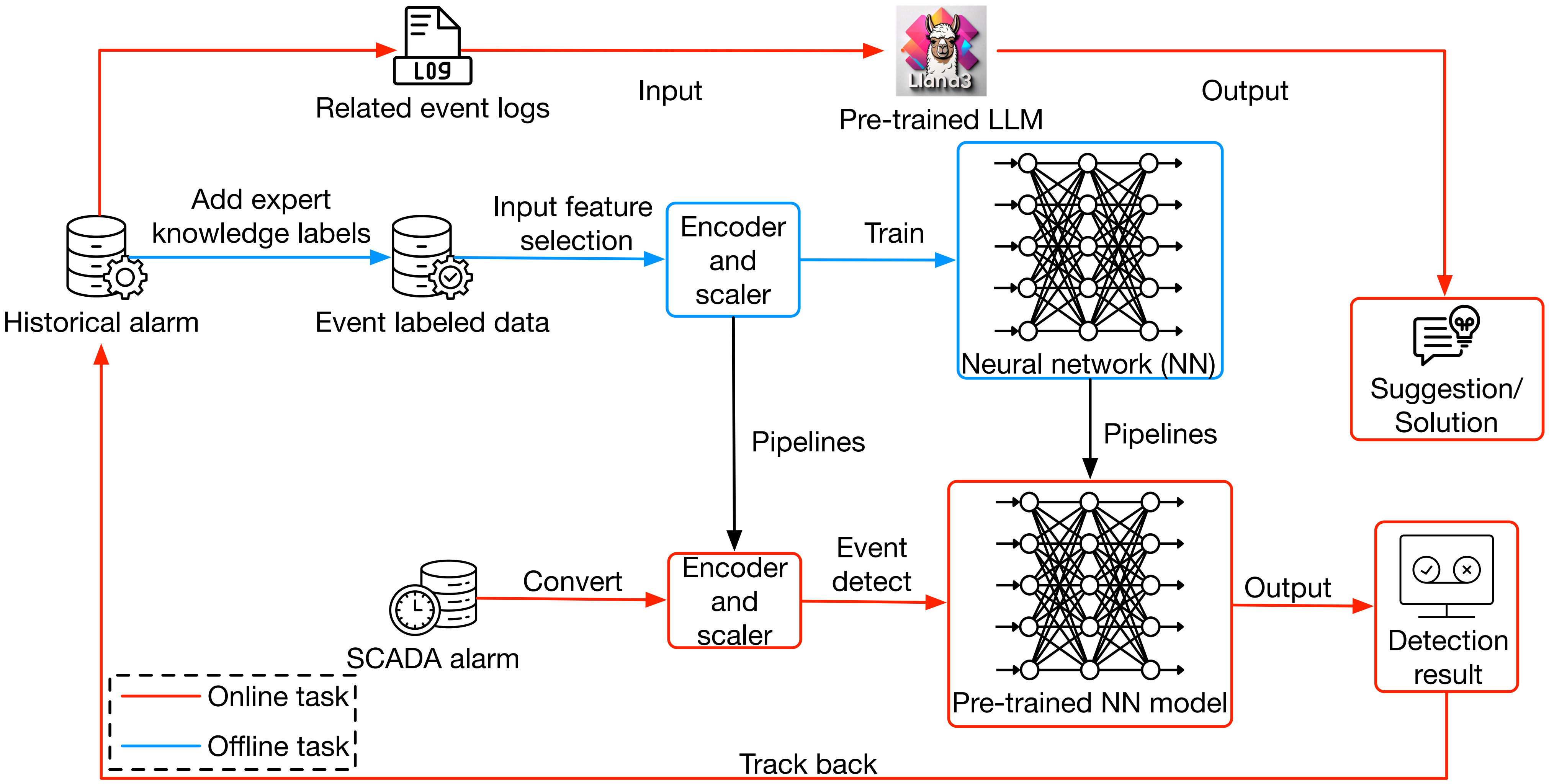
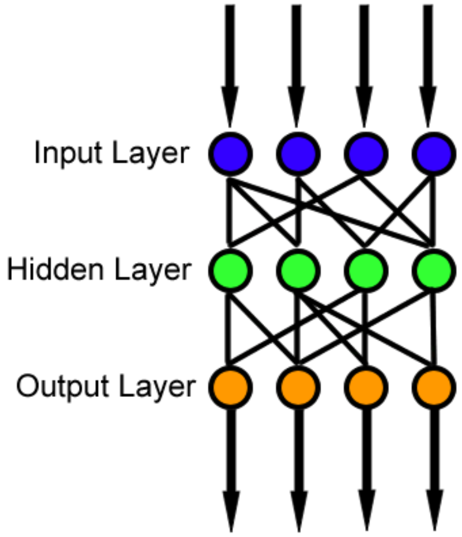


Fig. 2 The framework of developed alarm event detection system.

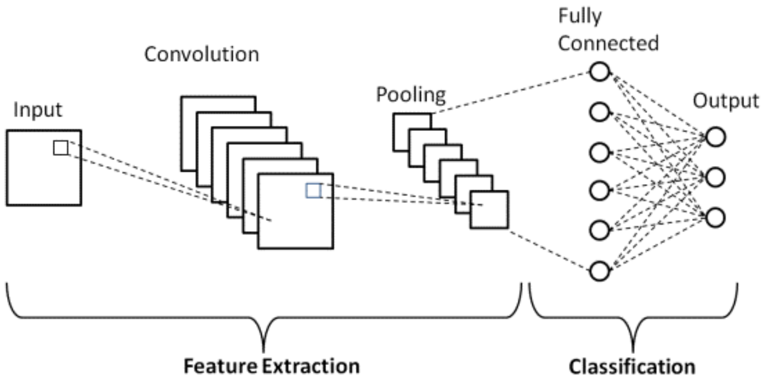
RMIT UNIVERSITY

Neural Network Comparison for SCADA Alarm Detection

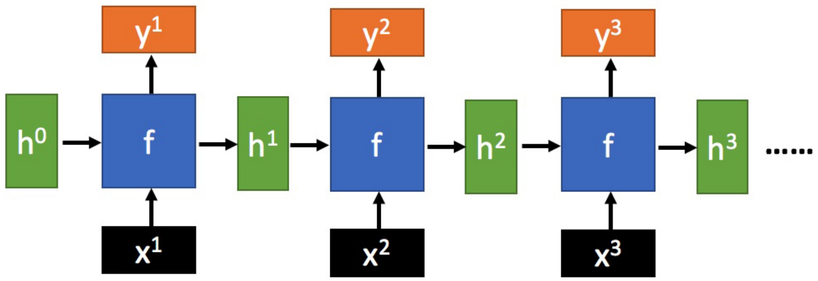
Architecture	Operation	Strengths	Limitations	Suitability for SCADA
FNN	Sequential processing, no data assumptions	Versatile, simple, scalable	Requires large data & time for training	**Best fit**
CNN	Pattern recognition in hierarchical layers	Great for feature extraction (images)	Not suitable for non-hierarchical data	**Not ideal**
RNN	Processes sequential data, maintains memory	Good for time-series & evolving data	Struggles with chaotic, unordered inputs	**Not suitable**



Feedforward Neural Network FNN



Convolutional Neural Network (CNN)



Recurrent Neural Network (RNN)

Alarm event decision support

- This distance measure serves as a generalized form encompassing both **Euclidean** and **Manhattan** distance metrics [9]

$$SD = \left(\sum_{i=1}^{n} |e_i - E_i| \right)^{1/p}$$

where e_i represents the detected alarm event, while E_i denotes a previous alarm event. The parameter p signifies the order of the norm.

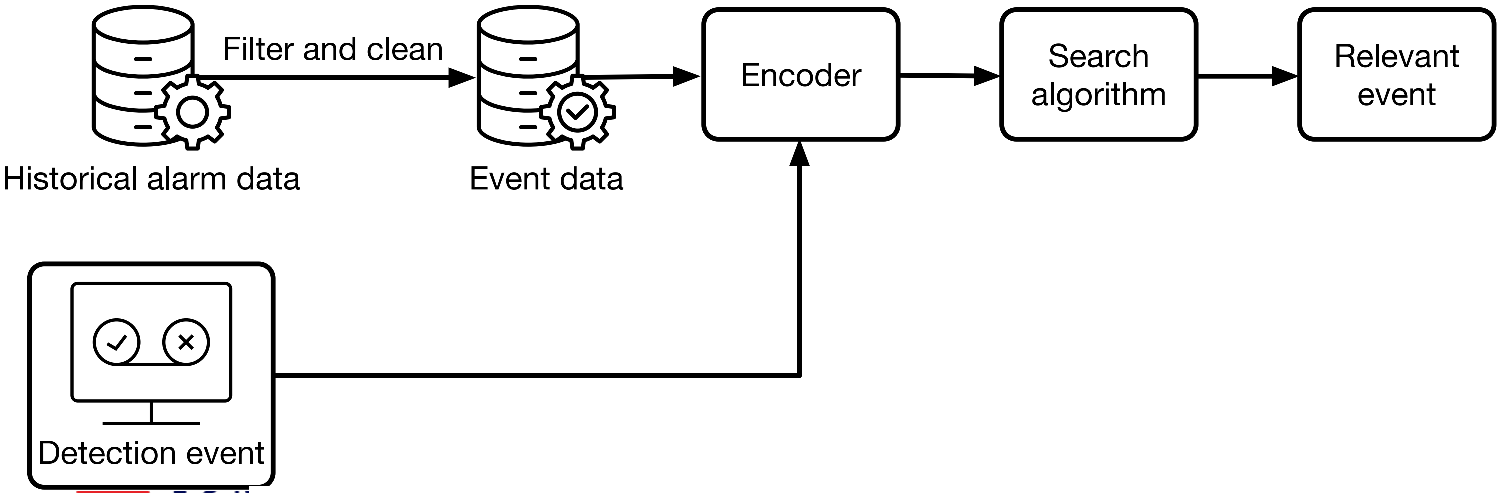


Fig. 3 The relevant alarm event searching process.

Algorithm 1. Historical Event Search and Decision Support

procedure
  Encoding input features of historical and detected events $\{\mathbf{E}, e\}$
  for Each historical event $E \in \mathbf{E}$ **do**
    Calculate SD between E and e by Eq.(5);
  end for
  Obtain minimal distance historical event E';
  Find the log of E'
  Input e, E', the log of E' to LLM
  Input related questions
  Return answers from LLM
end procedure

Empirical Study

- **Chattering event detection**
  - SCADA alarm data:
    - From May 1, 2017, to May 25, 2017.
    - Training set: from 00:00:00 on May 1, 2017, to 23:59:59 on May 24, 2017.
      - 2,572,919 chattering events and 2,132,938 non-chattering events.
    - Testing set: from 00:00:00 to 01:00:00 on May 25, 2017.
      - 3,717 chattering events and 3,035 non-chattering events.

	EventId	EventTimeStamp	SCADA_Category	TOC	AOR	Priority_Code	Substation	DeviceType	Device	event_message	chattering
0	26	2017-05-01 00:00:04	MH	TMS	TOCGR	3	Substation1002	RELAY	Device1089	#1 PRIMARY RELAY FAIL	1
1	45	2017-05-01 00:00:06	MH	TMS	TOCGR	3	Substation1002	RELAY	Device1089	#1 PRIMARY RELAY NORMAL	1
2	147	2017-05-01 00:00:47	MH	TMS	TOCGR	3	Substation1002	RELAY	Device1089	#1 PRIMARY RELAY FAIL	1
3	150	2017-05-01 00:00:49	MH	TMS	TOCGR	3	Substation1002	RELAY	Device1089	#1 PRIMARY RELAY NORMAL	1
4	108	2017-05-01 00:00:31	MH	TMS	TOCGR	3	Substation1002	RELAY	Device1090	#2 PRIMARY RELAY FAIL	0
5	125	2017-05-01 00:00:35	MH	TMS	TOCGR	3	Substation1002	RELAY	Device1090	#2 PRIMARY RELAY NORMAL	0
6	39	2017-05-01 00:00:05	MH	TMS	TOCGR	3	Substation1049	BLKCAR	Device643	SIGNAL RECEIVED NORMAL	0
7	18	2017-05-01 00:00:03	ML	TMS	TOCSR	4	Substation1051	BLKCAR	Device292	SIGNAL RECEIVED TRIP ENABLED	0

Empirical Study

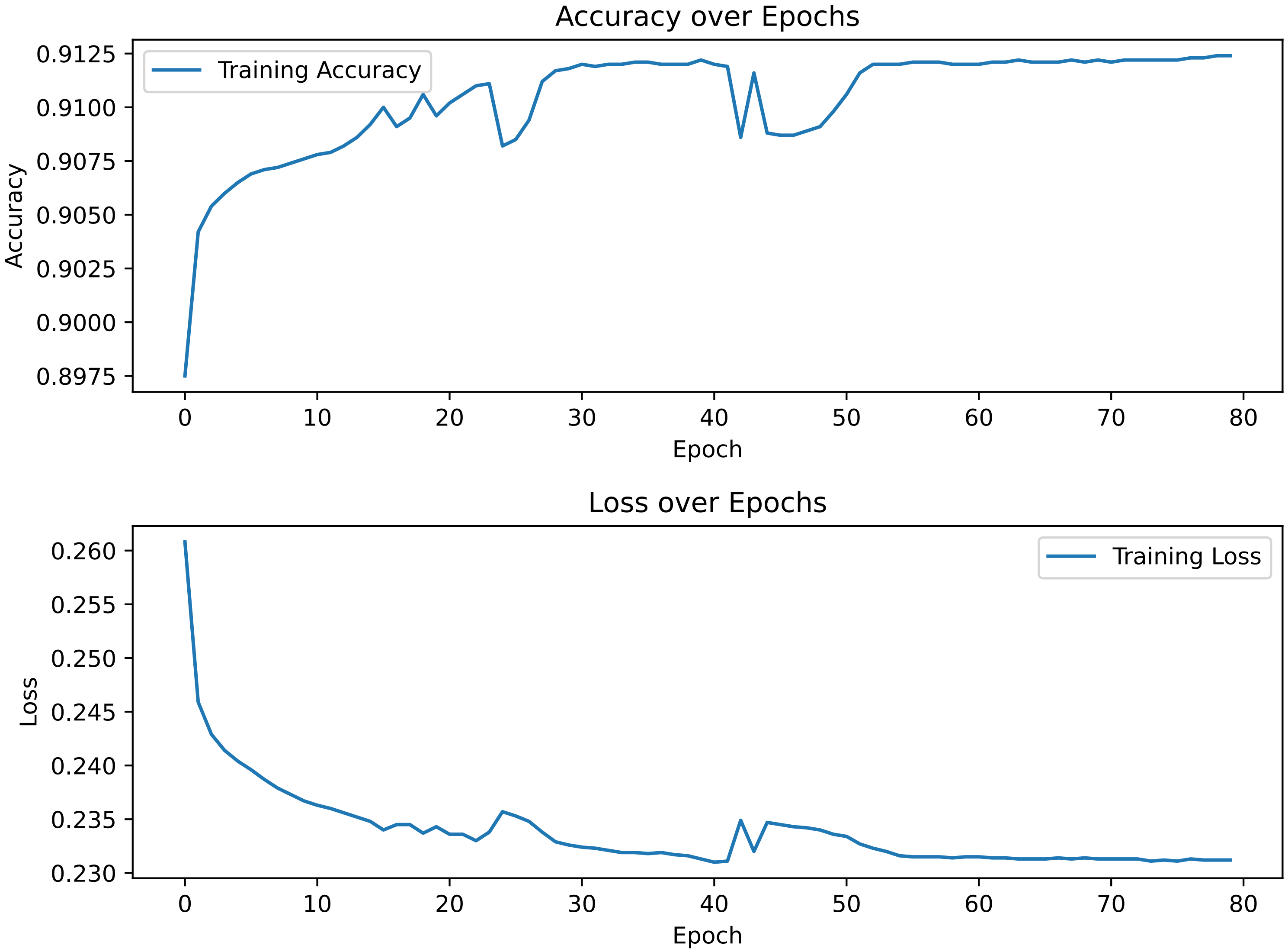


Fig. 4 The training accuracy and loss of proposed DNN

RMIT UNIVERSITY

Empirical Study

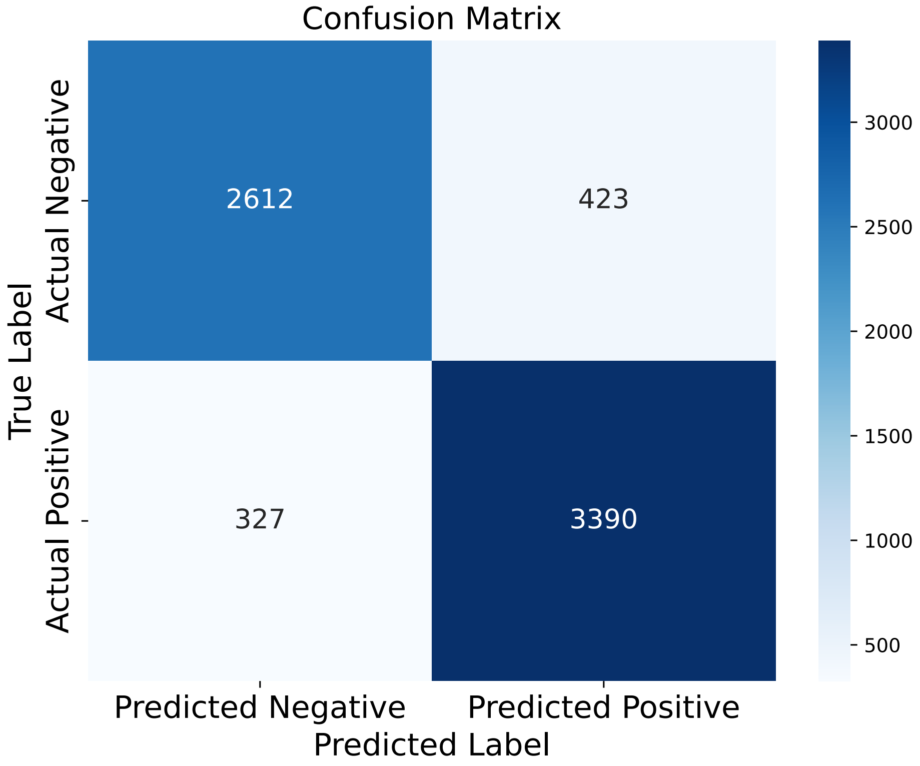


Fig. 5 The confusion matrix of testing data.

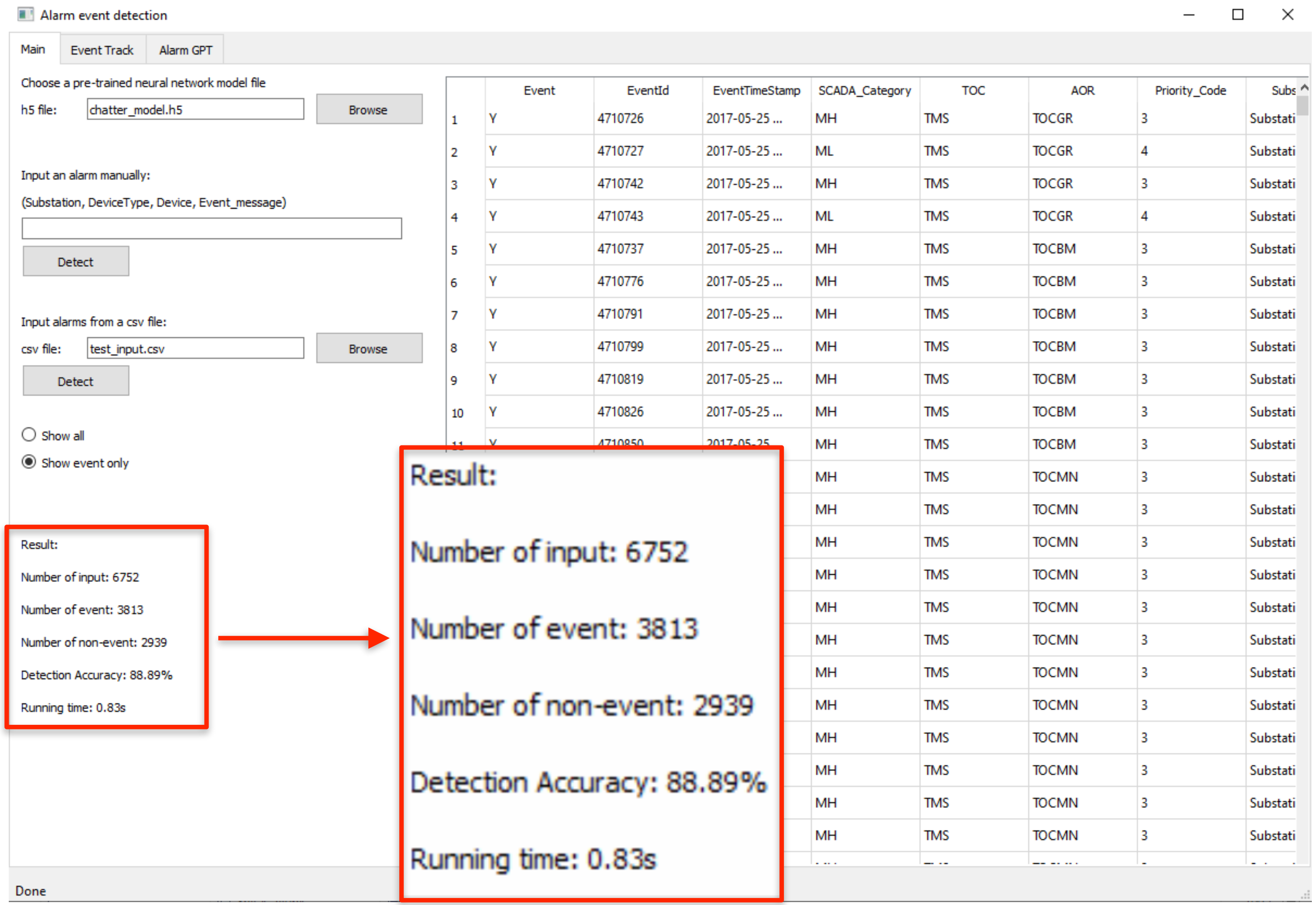
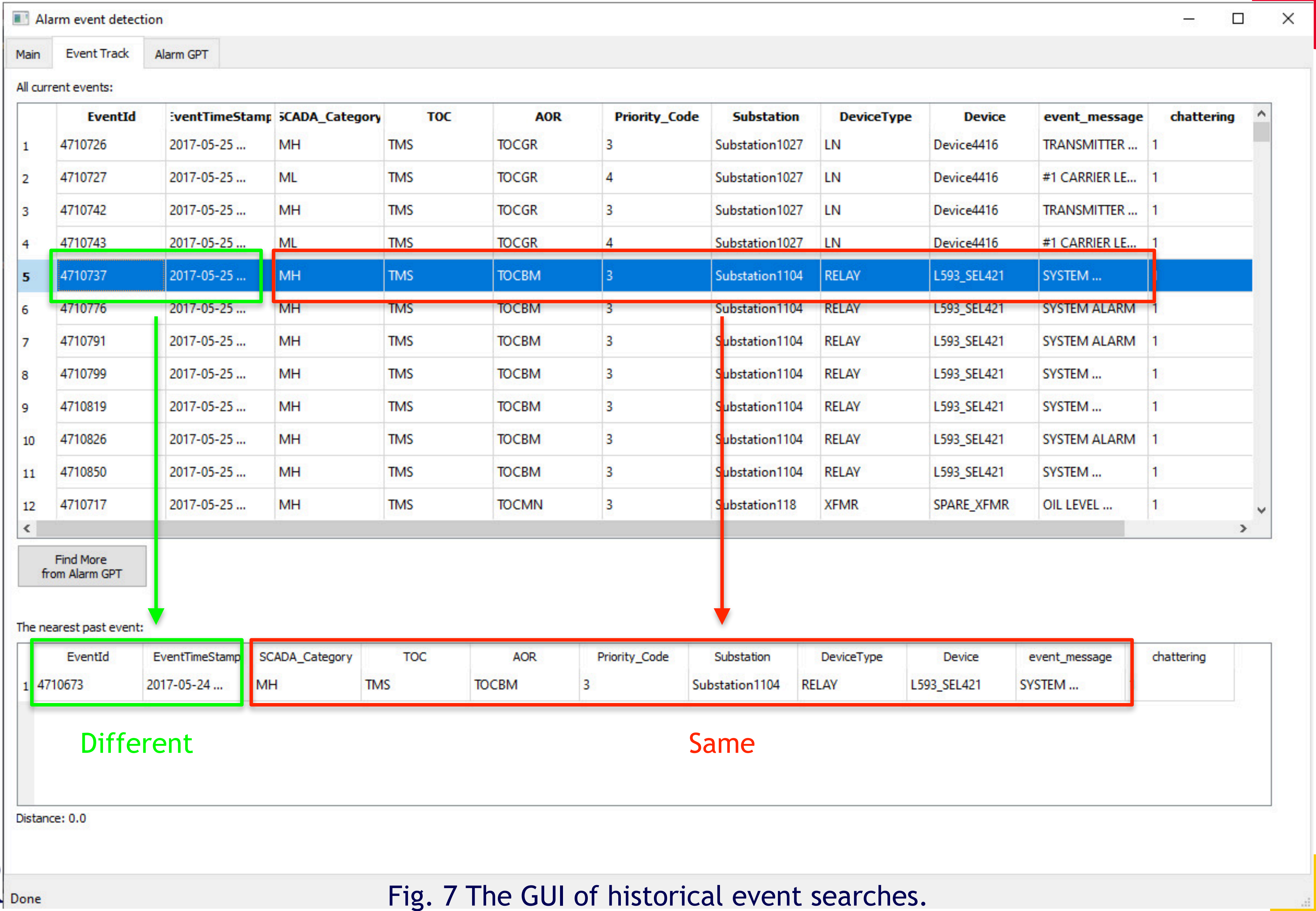


Fig. 6 The real-time SCADA alarm event detection.



	EventId	EventTimeStamp	SCADA_Category	TOC	AOR	Priority_Code	Substation	DeviceType	Device	event_message	chattering
1	4710726	2017-05-25 ...	MH	TMS	TOCGR	3	Substation1027	LN	Device4416	TRANSMITTER ...	1
2	4710727	2017-05-25 ...	ML	TMS	TOCGR	4	Substation1027	LN	Device4416	#1 CARRIER LE...	1
3	4710742	2017-05-25 ...	MH	TMS	TOCGR	3	Substation1027	LN	Device4416	TRANSMITTER ...	1
4	4710743	2017-05-25 ...	ML	TMS	TOCGR	4	Substation1027	LN	Device4416	#1 CARRIER LE...	1
5	4710737	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ...	
6	4710776	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ALARM	1
7	4710791	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ALARM	1
8	4710799	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ...	1
9	4710819	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ...	1
10	4710826	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ALARM	1
11	4710850	2017-05-25 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ...	1
12	4710717	2017-05-25 ...	MH	TMS	TOCMN	3	Substation118	XFMR	SPARE_XFMR	OIL LEVEL ...	1

	EventId	EventTimeStamp	SCADA_Category	TOC	AOR	Priority_Code	Substation	DeviceType	Device	event_message	chattering
1	4710673	2017-05-24 ...	MH	TMS	TOCBM	3	Substation1104	RELAY	L593_SEL421	SYSTEM ...	

Fig. 7 The GUI of historical event searches.

UNIVERSITY

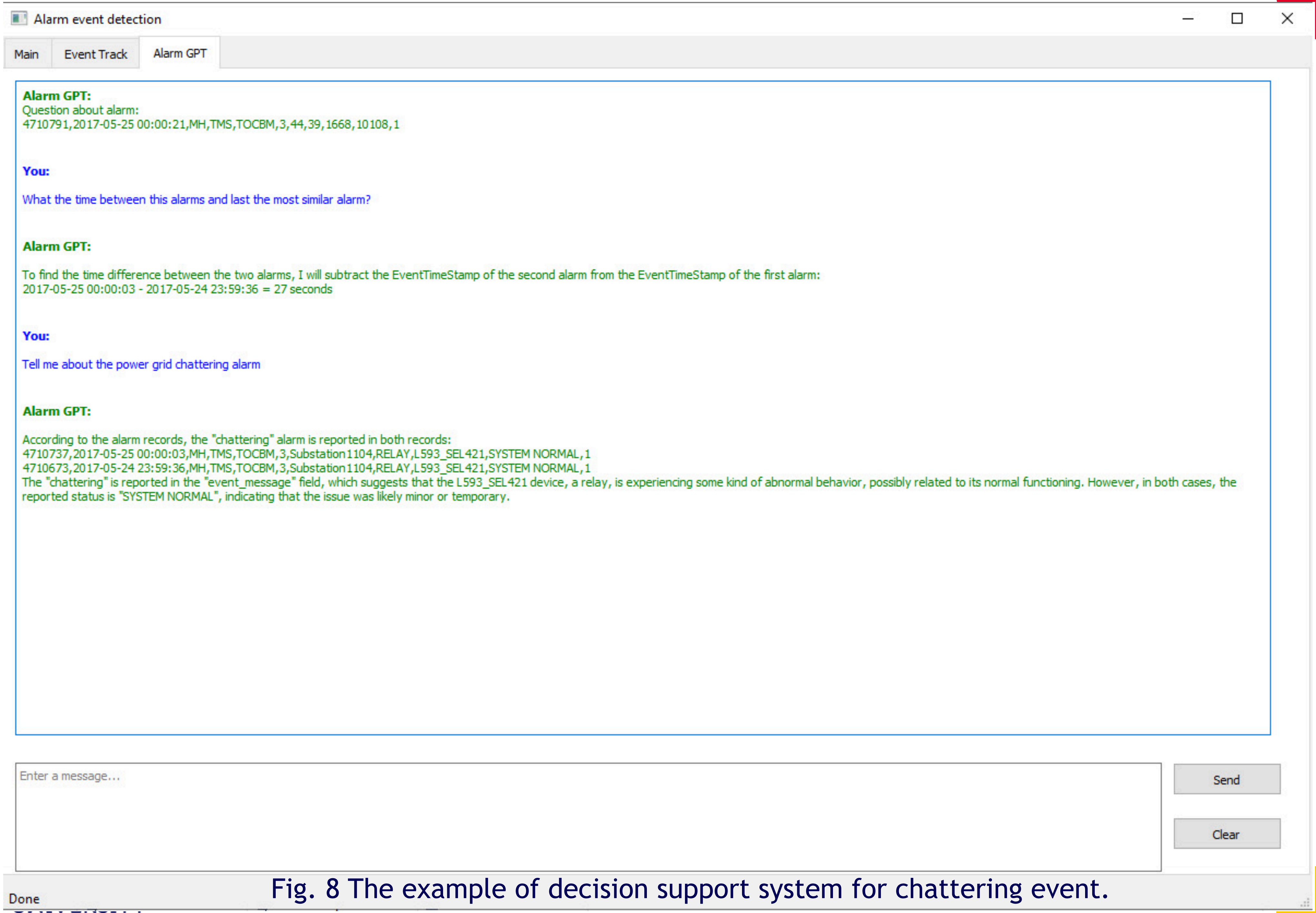


Fig. 8 The example of decision support system for chattering event.

Conclusion

- A real-time machine learning framework was developed specifically for SCADA alarm event detection.

- The introduction of a DNN architecture enhances the ability to efficiently detect real-time alarm events.

- A specialized algorithm for historically relevant event search supports decision-making.

References

[1] Bi, S. and Zhang, Y.J.A., 2017. Graph-based cyber security analysis of state estimation in smart power grid. *IEEE Communications Magazine*, *55*(4), pp.176-183.

[2] Tesch, D.B., Yu, D.C., Fu, L.M. and Vairavan, K., 1990. A knowledge-based alarm processor for an energy management system. *IEEE Transactions on power systems*, *5*(1), pp.268-275.

[3] Sun, G., Ding, X., Wei, Z., Shen, P., Zhao, Y., Huang, Q., Zhang, L. and Zang, H., 2019. Intelligent classification method for grid-monitoring alarm messages based on information theory. *Energies*, *12*(14), p.2814.

[4] Hor, C.L., Crossley, P.A. and Watson, S.J., 2007. Building knowledge for substation-based decision support using rough sets. *IEEE Transactions on Power Delivery*, *22*(3), pp.1372-1379.

[5] Sun, J., Qin, S.Y. and Song, Y.H., 2004. Fault diagnosis of electric power systems based on fuzzy Petri nets. *IEEE Transactions on Power Systems*, *19*(4), pp.2053-2059.

[6] Yongli, Z., Limin, H. and Jinling, L., 2006. Bayesian networks-based approach for power systems fault diagnosis. *IEEE Transactions on Power Delivery*, *21*(2), pp.634-639.

[7] Guo, W., Wen, F., Liao, Z., Wei, L. and Xin, J., 2009. An analytic model-based approach for power system alarm processing employing temporal constraint network. *IEEE Transactions on Power Delivery*, *25*(4), pp.2435-2447.

[8] Jiang, Y. and Srivastava, A.K., 2019. Data-driven event diagnosis in transmission systems with incomplete and conflicting alarms given sensor malfunctions. *IEEE Transactions on Power Delivery*, *35*(1), pp.214-225.

[9] Chiu, W.Y., Yen, G.G. and Juan, T.K., 2016. Minimum manhattan distance approach to multiple criteria decision making in multiobjective optimization problems. *IEEE Transactions on Evolutionary Computation*, *20*(6), pp.972-985.

Thanks for Listening

Questions?

RMIT
UNIVERSITY