Ontology-based Approach for Malicious Behaviour Detection in Synchrophasor Networks

Albalushi, A., Khan, R., McLaughlin, K., & Sezer, S. (2018). Ontology-based Approach for Malicious Behaviour Detection in Synchrophasor Networks. In *Proceedings of Power and Energy Society General Meeting (PESGM), 2017* (pp. 1-5). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/PESGM.2017.8274684

Published in:
Proceedings of Power and Energy Society General Meeting (PESGM), 2017

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
©2017 IEEE.
This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Open Access
This research has been made openly available by Queen's academics and its Open Research team. We would love to hear how access to this research benefits you. – Share your feedback with us: http://go.qub.ac.uk/oa-feedback

Download date:07. Aug. 2025

Ontology-based Approach for Malicious Behaviour Detection in Synchrophasor Networks

Abdullah Albalushi, Rafiullah Khan, Kieran McLaughlin and Sakir Sezer
Queen's University Belfast, Centre for Secure Information Technologies
Belfast BT3 9DT, United Kingdom
{aalbalushi01, rafiullah.khan, kieran.mclaughlin, s.sezer}@qub.ac.uk

***Abstract*—Synchrophasor systems are becoming a vital requirement for real-time monitoring, control and protection of emerging Smart Grids that need cyber security issues be carefully analysed and mitigated. This paper proposes a behaviour-based ontology on the Syncrophasor communications for the detection of malicious system behaviours. Syncrophasor activities are represented with their causal relationships using a flexible semantic model. The developed model bridges the gap between system behaviours and the exchanged data and commands in the network. A set of semantic rules are created to assist in identifying malicious activities that are deviating from the expected behaviour in the model. The proposed approach is prototyped and tested for its applicability in detecting cyber-attacks. Furthermore, a use case for valuable information extraction is described using query-based engine over the ontology knowledge. The presented results demonstrate the usefulness and flexibility of the proposed approach in detecting malicious activities that could improve Syncrophasor network security.**

I. Introduction

Phasor Measurement Units (PMUs) are time-synchronized devices that measure parameters of power quality such as voltages, currents, frequencies and phase angles in real-time. The measured data enable monitoring the performance and stability of power in the grid. Therefore, PMU (also known as Synchrophasor) plays a vital role in providing real-time monitoring, control and protection in future smart grids. PMU systems exchange their data over the IEEE C37.118 communication protocol which unfortunately does not provide any authenticity or encryption over the exchanged communications. This makes Synchrophasor exposed to several cyber-attacks [1] including Denial of Service (DoS) and Man in the Middle (MiTM) that could lead to severe time-delay or degradation in future smart grid control strategies that rely on Synchrophasor communications. Therefore, cyber security issues are considered a priority and need to be carefully analysed and mitigated.

This paper proposes an ontology-based approach for the analysis and monitoring of Synchrophasor systems to allow detection of malicious activities and cyber-attacks. In this approach, the characteristics of Synchrophasor communications are captured with their causal relationships using a flexible semantic model. The data extracted from the communications can be linked to real system behaviours, therefore, the gap between real system behaviours and exchanged data is bridged. A set of semantic rules were constructed to identify malicious activities that deviate from the expected behaviours in the model. The proposed approach is prototyped in Java and tested for its applicability using Man in the Middle attack scenario.

This work is mainly motivated by the attractive features of ontology that can enhance the information extraction and analysis in Synchrophasor networks. First, an ontology provides a flexible way in representing and processing large amount of data that could be produced by PMU systems at their high rate of transmission. The knowledge can be presented at various levels of abstraction and in easy machine-interpretable formats. Second, a rich set of semantic-level capabilities are made possible that includes mapping heterogeneous information sources obtained from both operational and non-operational prospective, extracting logical relationships between domain concepts, applying automated reasoning and contextual enhancement on the data. Despite the fact that benefits of ontology have been accepted and utilized in power system domain, its use is still limited and no research investigated applying ontology-based intrusion detection in IEEE C37.118 communications.

The reminder of this paper is organized as follows. Section II presents a brief background about Syncrophasor and summarizes recent work on ontology based systems. The proposed approach is presented in Section III. The experimental results on the proposed approach are presented in Section IV. Finally, Section V concludes the paper.

II. Related Work

A. Syncrophasor Technology

Syncrophasor technology is used for real-time operations and off-line engineering analyses to improve grid reliability and efficiency and lower the operational cost. Typically used technologies include Phasor Measurement Units (PMUs), Phasor Data concentrators (PDCs) and IT communication systems.

PMU devices measure the electrical waves on electricity grids that may be distributed over large geographical area. Each measurement is time-stamped using a common time source such as Global Positioning System (GPS) which allow time alignment on collected measurements for comprehensive view of the entire grid. On the other hand, PDCs gather measurement data from several PMUs with ability to filter out bad data before it can be transmitted to other information systems for monitoring and control purposes.

The typical flow between a PMU and a PDC over the IEEE C37.118 communication protocol is depicted in Figure

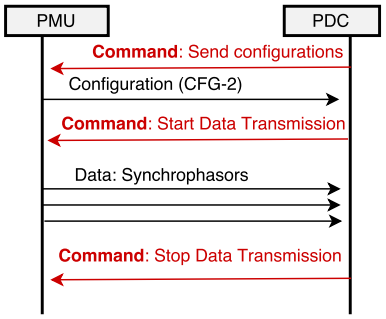

Fig. 1. Syncrophasor Communications Flow

1. The PDC instructs a PMU to send its configuration using the send configuration control command. The PMU respond with its configuration which provides description on how to decode exchanged measurement data. The PDC then instructs the PMU to start its data transmission that will take place until further command to stop transmission is received.

B. Ontology Approaches for Power System Networks

In recent years, the use of ontology in the electric power industry has received an increasing research attention. Ontology is an artificial intelligence technique that formally represents the concepts within a domain with their relationship. It enables powerful capabilities in controlling the level of details on information and automatically extracting, enhancing and analysing large amount of data. Several approaches with different applications of ontology were seen in power system domain that include system modelling, multi-type data management [2]–[4], big data analysis [5], [6], fault diagnosis [7], [8] and network security [9], [10].

In [10] an ontology-based approach on intrusion alerts is presented for the detection of cyber-attacks on SCADA systems. However, the presented ontology is focused on post-analysis of intrusion alerts and vulnerability information in SCADA networks and does not provide detection from raw network data.

Wang et. al [7] proposed an ontology-based fault diagnosis for power transformers. The presented ontology is used to integrate various transformers diagnostic information such as thermal condition monitoring, dissolved gas analysis, discharge and frequency response analysis for faults identification. Similarly, the work presented in [8] proposed a semantic information model for power grid fault diagnosis based on Common Information Model (CIM), that is based on IEC61850 communications.

The authors in [11] used an ontology based approach to reason about heterogeneous data sources to find ringlets in the power distribution network and detect power-transformer utilization for a given substation. In [9] the authors proposed an ontology-based framework for event understanding and representation in smart grids. The presented approach enables the extraction of high-level information from PMU data and evaluating semantic rules for the detection of basic events such as voltage level over a service area.

Supported by the increasing number of proposals on ontology-based systems in the power grid domain, it is clear that the importance and benefits of ontology in representing and analysing the knowledge within the domain are realized. However, no research has focused on utilizing ontology for intrusion detection in Synchrophasor network over IEEE C37.118 protocol. With its flexibility and reasoning capability over large amount of data, an ontology can provide a valuable contribution in detecting malicious Synchrophasor behaviours and enhancing the network security.

III. Proposed Approach

The proposed approach utilizes an ontology-based behaviour modelling of the Syncrophasor systems that use the IEEE C37.118 communication protocol. The developed ontology captures the domain knowledge about expected behaviours of the monitored systems and applies logical reasoning to recognise and classify malicious activities. More precisely, the capabilities and characteristics of PMU and PDC systems are monitored with a linkage to the exchanged data and control commands in the network. Furthermore, a set of detection rules are developed for the detection of malicious activities that does not match the defined characteristics of Syncrophasor systems in the ontology.

A. Behaviours Representation using Ontology

Syncrophasor systems are distinguished from traditional IT networks by their regularity of communications which includes a fixed number of devices and specific communication protocols. Each type of system may have a particular number of behaviours based on its role that may include the following:

A **PMU** can send its *header*, *configuration*, and *measurement data* to a PDC. Other behaviours that could be indicated by the exchanged data are *starting* or *stopping data transmission*, reporting *PMU errors* or *time synchronization issues*, transmitting *invalid data* or announcing *configuration changes* on PMU side.

A **PDC** may send various control commands to enable *header* and *configuration* retrieval, control *start* and *stop* of data transmission on PMUs.

The IEEE C37.118 protocol specifications [12] explicitly indicate that only measured and computed data shall be transmitted by a PMU. Any other information is to be only sent when requested. Furthermore, sending control commands is only allowed by PDC.

The developed ontology captures various system behaviours and their inter-relationship that are linked to the actual network communications. A high-level view of this ontology is depicted in Figure 2. In the ontology, PMU and PDC systems (concepts) are considered Synchrophasor equipments that have different characteristics and relationships to the exchanged data in the network over the IEEE C37.118 protocol. A **PMU** has **information** (*Header, Configuration and Measurement data*) that could be used by **behaviours** (*send header, send configuration, send measurements*) as response to **Control commands** (*request for header or configuration, instruction to start data transmission*) sent by a **PDC**.

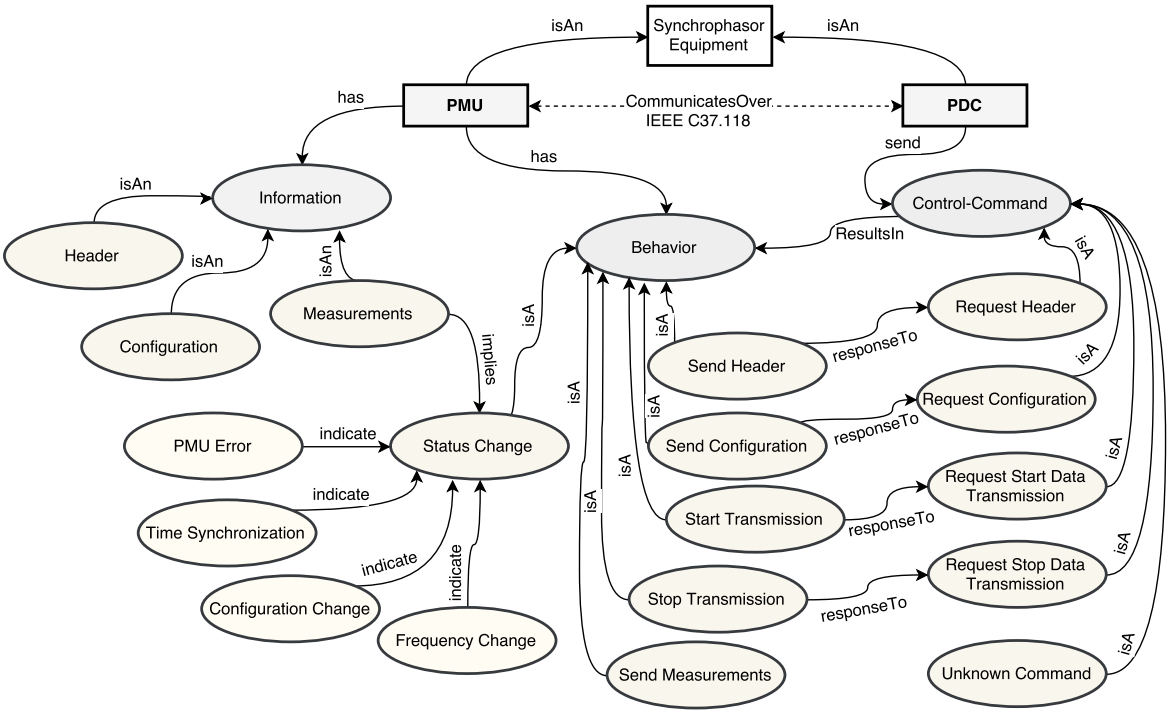

Fig. 2. Behaviour Ontology Model for Syncrophasor systems

B. Rule-base Construction

Rules play a very important role in ontology based systems. They can be constructed for different purposes such as mapping data to ontology, inferring concepts relationship, automating reasoning over acquired knowledge for context enhancement, and searching for specific information in the knowledge base.

In this paper, a set of rules was developed to identify suspicious system behaviours and cyber-attacks. These rules are constructed using the Semantic Web Rule Language (SWRL) and are evaluated against the raw network traffic represented in Resource Description Format (RDF). RDF is a standard used to describe data as triples that consists of Subject, Predicate, and Object. An excerpt of SWRL rules used within the ontology is presented in Table I. It should be noted that the presented rules are meant to describe how detection rules for various activities may be constructed. It is intended that further rules will be developed to capture other malicious activities with the Syncrophasor systems.

The presented detection rules in Table I provide the meaning to capture different suspicious activities of monitored systems. Rule 1 is triggered when a PMU system is attempting to send a control command which conflicts to the protocol specifications. Rules 2 to 5 concern monitoring the PMU system changes such as reported errors, time synchronisation issues, configurations and rate of transmission changes respectively. This information is extracted from the PMU data frames.

Furthermore, rules 6 to 8 enable the detection of suspicious devices that attempt first time communication to an existing system, injected configuration messages that does not match the expected sequence of configuration change count or the observed length over time, respectively. Finally, rule 9 allows easy identification of systems with more than one unique physical MAC address but pointing to the same IP address which indicates ARP spoofing attempt.

TABLE I
AN EXCERPT OF SWRL RULES USED WITHIN THE BEHAVIOUR ONTOLOGY

Rule Content
Rule1 := IsPMU(?m) ˆ SendControlCommand(?m, ?c) –>CompromisedPMU(?m)
Rule2 := IsPMU(?m) ˆ hasBehaviour(?b) ˆ hasStatusChange(?b, PMUerror) –>PMUwithError(?m)
Rule3 := IsPMU(?m) ˆ hasBehaviour(?b) ˆ hasStatusChange(?b, OutTimeSync) –>PMUSyncIssue(?m)
Rule4 := IsPMU(?m) ˆ hasBehaviour(?b) ˆ hasStatusChange(?b, ConfigChange) –>PMUConfigChange(?m)
Rule5 := IsPMU(?m) ˆ hasBehaviour(?b) ˆ hasStatusChange(?b, TransRateChange) –>PMUrateChange(?m)
Rule6 := IsPMU(?m) ˆ isPDC(?d) ˆ communicateWith(?m, ?d) ˆ ,FirstTimeCommunication(?m, ?d) –>NewDeviceCommunication(?m, ?d)
Rule7 := IsPMU(?m) ˆ sendConfiguration(?b, ?c) ˆ hasChangeCount(?c, ?h) ˆ swrlb:lessThan(?h, previousConfigChangeCount) –>SuspiciousConfiguration(?c)
Rule8 := IsPMU(?m) ˆ sendConfiguration(?b, ?c) ˆ hasLength(?c, ?l) ˆ lessThan(?l, previousConfigLength) –>SuspiciousConfiguration(?c)
Rule9 := IsDevice(?s) ˆ hasIPaddress(?s, ?ip) ˆ (hasMacAddress >=2) (?s) –>ARPspoofed(?s)

IV. Experimental Results

In order to test the proposed approach for malicious system behaviour detection, a prototype tool is developed on the open-source Jena API [13] in Java language. Jena provides a rich set of capabilities for processing ontology models and creating data instances that will be evaluated using the semantic detection rules. The research test-bed used for this paper, which is depicted in Figure 3, contains a local **PDC** (*IP:10.27.1.2, MAC:08:00:27:db:3a:a9*), **PMU**(*IP:10.27.1.55, MAC: 08:00:27:83:15:6a*), **Historian Database** and **Attacker system** (*IP:10.27.1.211, MAC:08:00:22:55:66:7a*). The open-source Synchrophasor simulator (OpenPDC [14]) is used for PMU and PDC traffic generation over the IEEE C37.118 protocol. The Man in the Middle and malicious packet injection attack is performed using pyPMU Python library for IEEE C37.118 and Metasploit [15] tools.

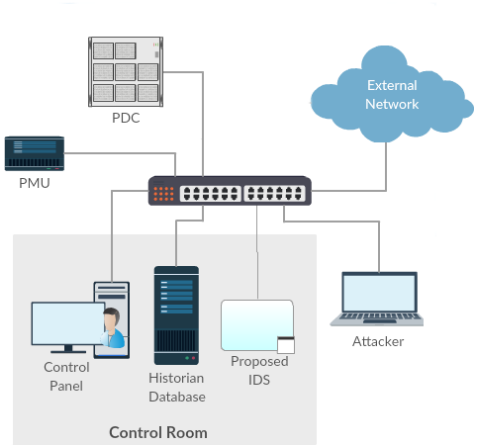

Fig. 3. High-level view of the test-bed architecture

A. Man in the Middle (MiTM)

The MiTM attack is a form of an active eavesdropping where an attacker can place himself in the middle of a PMU and a PDC communication. A common technique used to achieve this attack is the use of ARP spoofing. A successful MiTM attack gives the attacker almost full observation and control over the exchanged data which include the ability to manipulate real-time measurements, configurations and control commands.

The proposed system was successfully able to detect various malicious activities in the simulated attack scenario. For referencing purposes, each packet in the communication flow is assigned a unique packet identifier (e.g., C37PacketXXXX) by the proposed system. First, the ARP spoofing is detected by Rule 9 where a new MAC address *08:00:22:55:66:7a* (Attacker MAC) has been observed on a specific PMU system with IP address *10.27.1.55* as shown in Table II. As previous packets were monitoring and stored in the knowledge base, the count of MAC addresses can be useful for better judgement on which of the addresses can be considered malicious. Therefore, an alert can be generated as:

```
10/12-14:14:16.520000 [**] [RULE9] C37_ONTOLOGY_IDS:
Suspicious MAC address (08:00:22:55:66:7a) has been
observed for PMU system (10.27.1.55), possible ARP Spoofing
[Classification:Attempted-MiTM][Priority:1]{TCP:IEEEC37.118}
10.27.1.55:47122 -> 10.27.1.2:46864 (PDC44)
```

Second, the attacker proceeds in his attack by injecting data and configuration frames in the communications as presented in Table III. The attacker captured some data frames sent by the PMU and issued a control command to instruct the PMU in stopping its active data transmission (as observed in *C37Packet7730*). Then, an injected data frame (*C37Packet7731*) indicating PMU configuration change is sent by the attacker. The PDC responded by requesting the configuration of the PMU as seen in packet (*C37Packet7733*). This request was captured by the attacker and a malicious configuration frame is injected as a response (*C37Packet7735*). However, the system observed that the later configuration message contains a suspicious change counter and length compared to previously captured system communications. Therefore, an alert is generated as:

```
10/12-14:14:18.401603 [**] [*] C37_ONTOLOGY_IDS: Malicious
Configuration frame has been observed in combination
with spoofed data frame. Possible MiTM is in place.
[Classification:Attempted-MiTM][Priority:1]{TCP:IEEEC37.118}
10.27.1.55:47122 -> 10.27.1.2:46864 (PDC44)
```

In conclusion, the identified sequence of PMU system behaviour and communications is $\text{PMU}_{\text{Behaviour1}}$ = {*InActiveDataTransmission, StoppedDataTransmission, SentDataFrame, SentConfiguration, SentDataFrames*} which conflicts with the expected system behaviour where a PMU can not send data frames if it is already in an inactive transmission state.

B. Application on Behaviour Knowledge Extraction

The proposed approach could be also used for behaviour knowledge extraction in Synchrophasor networks. The extracted information may provide a valuable contribution for gaining in-depth understanding of system behaviours or to be used as pre-knowledge to intelligent data mining and machine learning algorithms. SPARQL [16] query language contains the required capabilities for information extraction which include querying RDF graphs with support to regular expressions and variables evaluation. Examples of information in Synchrophasor communications include, but not limited to, are the following:

- Which devices had communicated with a specific PMU over time?
- What commands have been sent towards a PMU (e.g., Send configuration, send header, start and stop of data transmission)?
- How many and which type of packets have been transmitted between two systems over a given time? *For detection of changes in rate of transmission caused by data injection attacks.*
- What packet lengths observed for every frame type used in PMU and PDC communications? *To detect possible over-sized packets.*
- Which PMU reported errors, time synchronization issues or changes in configuration or transmission rate?

TABLE II
ARP SPOOFING DETECTION BY FINDING DUPLICATED MAC ADDRESSES AND THEIR COUNTS

PacketID	Last Time-Stamp	SourceMAC	SourceIP	DestinationIP	DestinationSystem	Frame Types	Count
C37Packet7725	Oct 12, 2016 14:14:15.000000000 UTC	08:00:27:83:15:6a	10.27.1.55	10.27.1.2	PDC44	Data Frame	6716
C37Packet7731	Oct 12, 2016 14:14:16.520000000 UTC	**08:00:22:55:66:7a**	10.27.1.55	10.27.1.2	PDC44	Data Frame	1

TABLE III
MALICIOUS ACTIVITY SEQUENCES THAT INVOLVE DATA AND CONFIGURATION INJECTION ATTEMPTS

PacketID	Time-Stamp	SourceMAC	SourceIP	DestinationMAC	DestinationIP	FrameType	Config-Changed	Length
C37Packet7730	Oct 12, 2016 14:14:15.740030 UTC	**08:00:22:55:66:7a**	**10.27.1.211**	08:00:27:83:15:6a	10.27.1.55	Command Frame (Stop Data Transmission)		84
C37Packet7731	Oct 12, 2016 14:14:16.520000 UTC	**08:00:22:55:66:7a**	10.27.1.55	08:00:27:db:3a:a9	10.27.1.2	Data Frame	**Yes**	100
C37Packet7733	Oct 12, 2016 14:14:17.310023 UTC	08:00:27:db:3a:a9	10.27.1.2	08:00:22:55:66:7a	10.27.1.55	Command Frame (send CFG-2 frame)		84
C37Packet7735	Oct 12, 2016 14:14:17.564003 UTC	**08:00:22:55:66:7a**	10.27.1.55	08:00:27:db:3a:a9	10.27.1.2	ConfigV2 Frame		**460**

- Which execution sequences appeared in a PMU and PDC communication? *For detection of malicious sequences.*
- What PMU data (e.g., Frequency deviation from nominal) values have been reported over time and do they violate specified thresholds?

V. CONCLUSION

Synchrophasor systems are playing a vital role in wide-area monitoring, control and protection of emerging Smart Grids. However, a number of cyber security issues need to be carefully analysed and mitigated. This paper has proposed a novel approach based on ontology for malicious system behaviours detection in Synchrophasor network. The experimental results indicated that the proposed system can be implemented as an effective tool for the analysis and detection of abnormal behaviours. Ontology enables representing large volume of exchanged data that can be integrated and mapped to real behaviours of Synchrophasor systems in a machine-interpretable format. Furthermore, the powerful semantic-level capabilities such as automated reasoning, contextual enhancement and correlation over acquired knowledge make the ontology as an excellent potential for intelligent information analysis in the next generation IDSs. The presented ontology model will be updated by detailed PMU data definitions (e.g., Voltages and Frequencies) for extended system profiling and monitoring. For example, frequency deviation and voltage levels may be used for detection of an ongoing cyber attack such as measurement injection.

REFERENCES

[1] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, no. 3, p. 40, 2016.

[2] A. Pena and Y. K. Penya, "Distributed semantic repositories in smart grids," in *2011 9th IEEE Industrial Informatics*. IEEE, 2011, pp. 721–726.

[3] Q. Zhou, S. Natarajan, Y. Simmhan, and V. Prasanna, "Semantic information modeling for emerging applications in smart grid," in *2012 ITNG International Conference*. IEEE, 2012, pp. 775–782.

[4] D. Schachinger, W. Kastner, and S. Gaida, "Ontology-based abstraction layer for smart grid interaction in building energy management systems," *Proceedings of the IEEE*, pp. 1–6.

[5] Y. Huang and X. Zhou, "Knowledge model for electric power big data based on ontology and semantic web," *CSEE Journal of Power and Energy Systems*, vol. 1, no. 1, pp. 19–27, 2015.

[6] H. Yan-Hao, L. Wen-Chen, L. Bai-Qing, L. Ya-Lou, Z. Xiao-Xin, and A. Ning, "The construction of power system knowledge database based on ontology theory and semantic web technology," in *POWERCON, 2014 International Conference on*. IEEE, 2014, pp. 1760–1764.

[7] D. Wang, W. Tang, and Q. Wu, "Ontology-based fault diagnosis for power transformers," in *IEEE PES General Meeting*. IEEE, 2010, pp. 1–8.

[8] Q. Lijun, H. Cuijuan, J. Huawei, and L. Meng, "Information model for power grid fault diagnosis based on cim," in *2011 4th International Conference on DRPT*. IEEE, 2011, pp. 866–870.

[9] C. Basu, A. Agrawal, J. Hazra, A. Kumar, D. P. Seetharam, J. Béland, S. Guillon, I. Kamwa, and C. Lafond, "Understanding events for wide-area situational awareness," in *2014 IEEE PES ISGT*. IEEE, 2014, pp. 1–5.

[10] D. Krauß and C. Thomalla, "Ontology-based detection of cyber-attacks to scada-systems in critical infrastructures," in *DICTAP, 2016*. IEEE, 2016, pp. 70–73.

[11] A. Zinflou, M. Gaha, A. Bouffard, L. Vouligny, C. Langheit, and M. Viau, "Application of an ontology-based and rule-based model in electric power utilities," in *2013 IEEE ICSC*. IEEE, 2013, pp. 405–411.

[12] K. Martin, G. Brunello, M. Adamiak, G. Antonova, M. Begovic, G. Benmouyal, P. Bui, H. Falk, V. Gharpure, A. Goldstein *et al.*, "An overview of the ieee standard c37. 118.2synchrophasor data transfer for power systems," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1980–1984, 2014.

[13] B. McBride, "Jena: A semantic web toolkit," *IEEE Internet computing*, vol. 6, no. 6, p. 55, 2002.

[14] G. P. Alliance, "openpdc," *Available on-line: http://openpdc.codeplex.com*, 2011.

[15] D. Maynor and T. Wilhelm, "Metasploit toolkit for penetration testing, exploit development, and vulnerability research," 2007.

[16] E. PrudHommeaux, A. Seaborne *et al.*, "Sparql query language for rdf," *W3C recommendation*, vol. 15, 2008.