Detecting Attacks in Electric Power System Critical Infrastructure Using Rough Classification Algorithm

Maurĭio Pereira Coutinho, Germano Lambert-Torres, *Member,* IEEE,
Luiz Eduardo Borges da Silva, *Member,* IEEE, and Horst Lazarek

***Abstract*— This paper presented an alternative technique to improve the security of Electric Power Control Systems by using anomaly detection to identify attacks and faults. By using Rough Sets Classification Algorithm, a set of rules can be defined. The alternative approach tries to reduce the number of input variables and the number of examples, offering a more compact set of examples in order to fix the rules to the anomaly detection process. An illustrative example is presented.**

***Index Terms*—Electric power system, detecting attacks, rough set theory, data mining.**

I. Introduction to Critical Infrastructures

NOWADAYS, Critical Infrastructure plays a fundamental role in our modern society. Telecommunication and transportation services, water and electricity supply, and banking and financial services are examples of such infrastructures that provide critical services to our communities. The interconnection of such structures and the use of information technology in order to achieve quality of their services expose the society to more vulnerabilities and security threats. With a computer and an Internet connection, intruders can remotely access interconnected and interdependent Critical Infrastructures to interrupt important services. To safeguard against the threat of such cyber-attacks, providers of Critical Infrastructure services also need to maintain the accuracy, assurance and integrity of their interdependent data networks.

In United States of America, Critical Infrastructures are defined according the USA Patriot Act of 2001 as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national health or safety, or any combination of those matters*". The following Critical Infrastructure Sectors are identified in [1]: *Agriculture and Food, Banking and Finance, Chemicals and Hazardous Materials, Defence Industrial Base, Emergency Services, Energy, Higher Education, Insurance, Law Enforcement, Oil and Gas, Postal and Shipping, Public Health, Telecommunications and Information Technology, Transportation, Water, Commercial Key Assets, Dams, Governments Facilities, National Monuments and Icons, Nuclear Power Plants*. Accordingly to [2], a Critical Infrastructure can be divided into the following three layers: physical layer, cyber layer, and human operations layer. In the past, physical and human operations layers have been more vulnerable to attacks. Nowadays, we are seen the increase in the vulnerability of the cyber layer.

Manuscript received September 24, 2006. This work was supported in part by the Brazilian Research Council (CNPq) and Minas Gerais State Research Foundation (FAPEMIG).

M. P. Coutinho, G. Lambert-Torres, and L.E. Borges da Silva are with the Federal University of Itajuba (UNIFEI), Itajuba, MG, 37500-503, Brazil (phone: +55-35-36291240; fax: +55-35-3629118755; e-mail: {coutinho, germanoltorres}@gmail.com).

H. Lazarek is with the Technical University of Dresden, Dresden, Germany.

II. Initiatives for Security of Critical Infrastructure

Guidance documents, standards, legislations, and regulations in order to improve security of Critical Infrastructures are currently in development around many countries. The initiatives differ with respect to the involved parties and their goals, as well as geographic and industry scope [3]. This section presents some of those initiatives.

Since September, 11, 2001 terrorism and homeland security have taken top priority in U.S. governmental policy and affairs. Examples can be found in the release of "The National Strategy to Secure Cyberspace" [4] and with the official creation of the Department of Homeland Security (DHS) [5]. An initiative of the Eidgenössische Technische Hochschule Zürich (ETHZ) and other partners is "The International Critical Information Infrastructure Protection (CIIP) Handbook" [3] that surveys critical information infrastructure protection efforts in fourteen countries. The main focus is on the national governmental efforts to protect critical information infrastructures. The IT Baseline Protection Manual is a German initiative of the Bundesamt für Sicherheit in der Informationstechnik (BSI) and it recommends a series of standard security measures for typical IT applications and IT systems [6]. In the area of evaluating computer systems and software from a security perspective there are the Trusted Computer System Evaluation Criteria (TCSEC), or the Orange

book, the Information Technology Security Evaluation Criteria (ITSEC), the Common Criteria for Information Technology Security Evaluation (CCITSE)] or ISO/IEC 15408. Another initiative is the "Process Control Security Requirements Forum (PCSRF)", which is a industry group working with security professionals to assess vulnerabilities and establish appropriate strategies for the development of policies to reduce IT security risk within the US process control industry [7]. The ISA Committee SP99 "Manufacturing and Control Systems Security" intends to create guidance documents and a Standard (S99) on introducing IT security to existing industrial control and automation systems [8]. The objective for this IEC standard is to describe state-of-art secure realization of certain common automation networking scenarios [9]. The British Columbia Institute of Technology (BCIT) maintains an Industrial Cyber Security Incident Database, designed to track incidents of a cyber security nature that affect industrial control systems and processes [10].

III. Security Fundamentals

The security objectives offer a framework for categorizing and comparing the security mechanisms of various systems. They are: Confidentiality, Integrity, Availability, Authentication, Authorization, Auditability, Nonrepudiability, and Third-Party Protection. An intentional violation of a security objective is called attack. Attacks may either be initiated by persons outside or by insiders. Some common types of attacks are the following: Denial of Service, Eavesdropping, Spoofing, Man-in-the-Middle, Breaking into system, Virus, Trojan, and Worm [11]. Naedele and Dzung [12] enumerate a relationship between the security objective and the security mechanism.

In [13], it is showed how the increasing sophistication of attacks from the mid-1980s to the present have grown in complexity and in automation in despite of the skill required to launch the attacks has been reduced. This is an indication that this automation may be the trigger for large-scale activity on the internet.

IV. Electric Energy Critical Infrastructure

The Electric Utility Information Technology Systems can be divide in four kinds: Business Computers, Engineering Computers, Control Centre Computers, and Embedded Computers [14]. The use of Information Technology in the Control Centre Computers and Embedded Computers started, approximately, 3 decades ago. The operational structure used for this is based on data validation/conformation process to the supervisory and control system. This process is realized in 3 steps: Data Acquisition, Data Conditioning and Data Conversion. After this the data is inserted into the control and/or supervisory computer, where the specific treatment is accomplished and the actions are taken in order to maintain the behaviour and reliability of the system. See Fig. 1.

In general, a Electricity Cyber Infrastructure is highly interconnected and dynamic, consisting in several utilities. Due to its hierarchical organization, it is sub-divided into regional grids. Each sector is further split into generation, transmission, distribution and customer service systems, supplemented with an energy trading system. The Power Grid is comprised of a myriad of assets, such as Generation Plants, Transmission Lines, Transmission and Distribution Power Substations, Local, Regional and National Control Centres, Remote Terminal Units (RTUs)/Intelligent Electronic Devices (IEDs), and Communication Links [15].

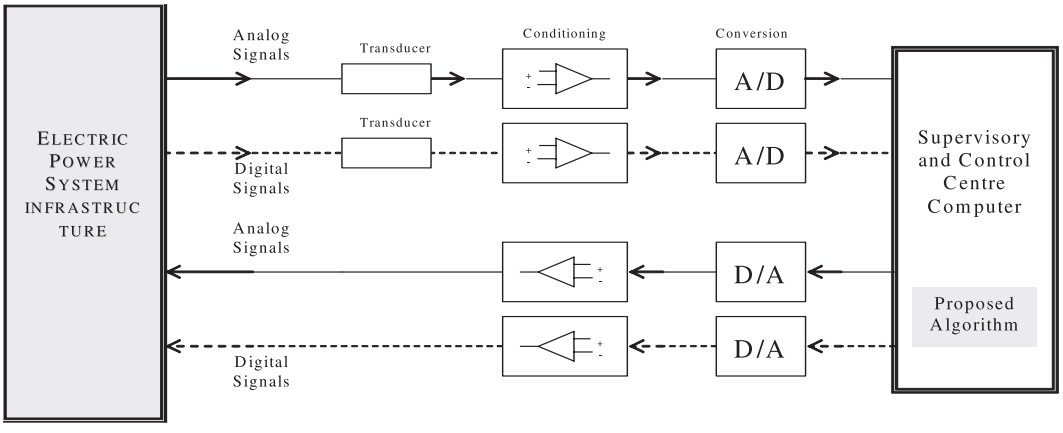

Fig. 1. Basic Block Diagram for a Digital Control System

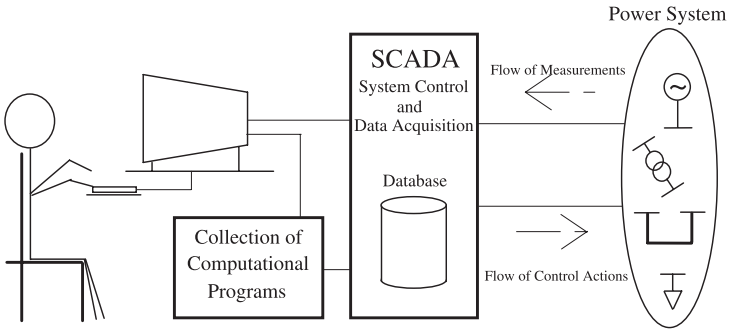

Fig. 2) Electricity cyber infrastructure.

The computer electricity cyber infrastructure can be divided in 2 parts: Electric Management Systems, which allow operators to regulate power flow, and the Supervisory Control and Data Acquisition (SCADA) systems for monitoring the safety, reliability, and protective functions of the power grid [15]. See Fig. 2.

V. Vulnerabilities in Electric Power Systems

Nowadays SCADA systems are an important part of the nation's Critical Infrastructure. They require protection from a variety of threats and their network are potentially vulnerable to cyber attacks because the proprietary protocols and networks have long been considered immune to attacks and security has not been part their design. The diversity and lack of interoperability in these communication protocols create obstacles for anyone attempting to establish a secure communication. The variety of communications media used to establish the communication links contributes for increasing of the infrastructure vulnerability [16].

VI. Detecting Attacks

Attacks on computer and network systems have significantly increased in recent years [12]. An intrusion Detection System (IDS) is a "burglar alarm" and has been widely studied in recent years, as in [17-20]. An extended bibliography can be found in [21]. IDSs can be characterized by different monitoring and analysis approaches. They can monitor events at three different levels: network, host, and application. These events can be analysed using two techniques: signature detection and anomaly detection. Anomaly-based IDSs find attacks by identifying unusual behaviour (anomalies) on a host or network. They function on the observation that some attackers behave differently than "normal" users and thus can be detected by systems that identify these differences. The measures and techniques used in anomaly detection include: Threshold detection, Statistical measures, and Rule-based measures [19]. Examples of anomaly detection techniques are IDES [22] and EMERALD [23].

VII. Previous Work

Different approaches have been used in the area of detecting intrusions in computer systems over the past 20 years. Most previous work on anomaly intrusion detection has determined profiles for user behaviour. Intrusions are detected when a user behaves out of character. These anomalies are detected by using statistical profiles, as in IDES [22], inductive pattern generation or neural networks as in [24, 35]. Manikopoulos and Papavassiliou [26] used statistical models using metrics derived from observation of the user's actions. Fink et al [27] focused on determining normal behaviour for privileged process, those that run as root. Another approach took from [24] it is similar to the later but it differs in that they use a much simpler representation of normal behaviour. Anomaly detection schemes also use data mining techniques such as clustering, support vector machines (SVM), and different neural network models. For example, Mukamala [28] describes approaches to intrusion detection using neural networks and SVM. Sekar et al [29] presented an approach that combines specification-based and anomaly-based intrusion detection, mitigating the weaknesses of the two approaches while magnifying their strengths. In [30], a novel multilevel hierarchical Kohonenen Net (K-Map) is introduced. Each level of the Hierarchical Map is modelled as a simple winner-take-all K-Map. The objective was to detect as many different types of attacks as possible. In [31], it is presented a data mining algorithm based on supervised clustering to learn patterns and use these patterns for data classification. In [32], it is presented research results on the detection of network security attacks in computer and control systems through the identification and monitoring of a synthetic "DNA Sequence". Just as DNA characterizes the make up of the human body a "DNA Sequence" of a computer system has similar functions. Changes in behavioural patterns of a computer system, such as virus attacks, are reflected in changes in the DNA Sequence and appropriate actions can be taken. Martinelli et al [33] proposed an approach to monitor and protect Electric Power System by learning normal system behaviour at substations level, and raising an alarm signal when an abnormal status is detected; the problem is addressed by the use of auto-associative neural networks, reading substation measures.

Wang et Battiti [34] proposed a real time network based intrusion identification model based on Principal Component Analysis (PCA). The PCA technique is used to profile normal program and user behaviours for host-based anomaly intrusion detection. Song et al [35] introduces the Hierarchical Random Subset Selection-Dynamic Subset Selection (RSS-DSS) algorithm for dynamically filtering large data sets based on the concepts of training pattern age and difficult, while utilizing a data structure to facilitate the efficient use of memory hierarchies. In [36], it is showed how the accuracy and security of SCADA Systems can be improved by using anomaly detection to identify bad values caused by attacks and faults. The performance of invariant induction and n-gram anomaly-detectors is compared.

VIII. Problem Definition

The operation of a power system is intrinsically complex due to the high degree of uncertainty and the large number of variables involved. The various supervision and control actions require the presence of an operator, who must be capable of efficiently responding to the most diverse requests, by handling various types of data and information.

These data and information come from measurements of SCADA systems or from computational processes. The size of the current database in a power control center has increased a lot in the last years due to the use of network communications. This makes their control systems more vulnerable to manipulation by malicious intruders. In order to improve the security of SCADA systems, anomaly detection can be used to identify corrupted values caused by malicious attacks and faults.

The aim of this paper is to present an alternative technique for implementing anomaly detection to monitor Power Electric Systems. The problem is addressed here by the use of Rough Sets Classification Algorithm, proposed by Pawlak in [37]. Related work can be found in [2, 33, 36, 38, 39].

The system operator needs to know the current state of the system and some forecasted position, such as load forecasting, maintenance scheduling, and so on in order to take a control action (switching, changing taps and voltage levels, and so on). One of the most important operator tasks is to determine the current operational state of the system. To accomplish this task, the operator receives many data from/into the system. By handling these data, the operator tries to build an image of the operation point. Fig.3 shows a representation of this process.

The analysis tries to make an assessment of the operational mode in one of the 2 states: normal, or abnormal. In the first state, normal, all loads are supplied and all measurements are inside of the nominal rates. In the second state, abnormal, all loads continue to be supplied but some of the measurements are outside the nominal rates or some loads are not supplied, i.e., there was a load shedding process.

Even when the operation state is normal, the operator needs to analyze the system security. This analysis is made according to possible contingencies that could affect the power system. Loss of a transmission line, shut down of a power plant or an increase of the load are some contingencies that can occur during the operation. An example of normal or abnormal points is shown in Fig. 3. It shows the same contingency for two different operation points. For the operation point A, the contingency produces an abnormal operation point; while for the operation point B, the system continues in the normal state. Thus, the point A is an unsafe operation point and point B is a safe one.

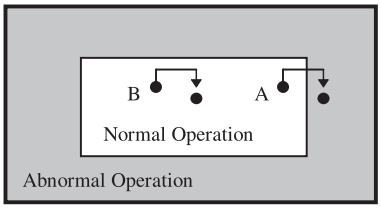

Fig. 3. Operational State of a Power System and Changing of Operation Point

The illustrative example that follows has an objective to describe the fundamentals concepts of the rough set theory applied to anomaly detection. The idea is to transform a set of examples in a set of rules that identify possible intruders. For sake of explanation, some assumptions and reductions are made. This approach gives the opportunity to detail each step of the formulation without reducing generalization.

IX. Description of the Problem

The main purpose of the illustrative example that follows is to help the understanding of the rough set theory fundamental concepts. The idea is to transform a set of examples in a set of rules that represent the operational state of a power system. Some assumptions and simplifications are made to allow a better understanding of each step of the formulation without loss of generality. In fact, the data used in this paper comes from a Brazilian electricity utility.

Consider a control center database composed by a set of measurements, such as the one shown in Table I. The operational state of the hypothetical power system depends on four elements: status of circuit-breaker A, transmission capacity of lines B and C, and voltage of bus D. Moreover, Table 1 contains the attributes represented by the set {A, B, C, D} and the corresponding decision S, where:

- the status of circuit-breaker A is defined by 0 (close) or 1 (open);
- the values of transmission lines B and C are percentages of real power flows according to their maximum capacities, in [%]; and,
- the bus voltage D is expressed as a fraction of the rated voltage.

The classification of each state is made according to an expert (usually, a senior operator/engineer), and four possible outputs can be selected for the power system operational state:

Normal or safe (S) or abnormal or unsafe levels 1,2 and 3 (L1, L2, L3, respectively). These levels can represent malicious actions in SCADA systems performed by the attackers like changing data values, changing information control, opening breakers, fraud, and overload.

TABLE I
REDUCED CONTROL CENTER DATABASE

	Attributes				
U	**A**	**B**	**C**	**D**	**S**
1	0	57	82	1,07	L2
2	0	37	32	0,97	L1
3	1	0	87	0,95	L3
4	1	72	31	1,07	L3
5	0	28	39	1,02	L1
6	0	42	82	1,07	L2
7	0	52	59	1,01	S
8	1	62	67	1,04	L3
9	0	57	45	0,99	S
10	0	45	58	1,00	S
11	0	32	57	0,94	S
12	0	0	57	1,08	L2
13	1	58	87	1,03	L3
14	0	58	56	1,07	L2
15	0	25	57	1,03	S
16	0	56	54	1,08	L2
17	1	59	72	1,08	L3
18	0	32	0	0,93	L1
19	0	32	45	0,94	S
20	1	72	67	0,96	L3
21	0	57	45	1,01	S
22	0	32	45	0,94	S
23	0	29	43	1,08	L2
24	1	0	72	0,95	L3
25	1	57	79	1,07	L3
26	0	31	43	0,99	S
27	0	32	42	0,94	S
28	0	17	32	0,92	L1
29	0	23	22	1,00	L1
30	0	23	57	0,91	S

Observing the above set of examples, it is really hard to conclude that the condition of transmission line B is not necessary in the classification process. Notice that, this attribute is a dispensable one, as shown later. Even in this very small database it is very hard to reach a conclusion. For real control center database, usually with hundreds important attributes and thousands of examples, it could be impossible to take a reliable control action.

X. PRESENTATION OF THE ALGORITHM

Before the presentation of the algorithm, two major concepts in Rough Set theory, *reduct* and *core*, will be defined. These concepts are important in the knowledge base reduction.

Let **R** be a family of equivalence relations. The reduct of **R**, *RED*(**R**), is defined as a reduced set of relations which conserve the same inductive classification of set **R**. The core of **R**, *CORE*(**R**), is the set of relations which appear in all reduct of **R**, i.e., the set of all indispensable relations to characterize the relation **R**. The main idea behind the knowledge base reduction is a simplification of a set of examples. This can be obtained by the following procedure:
a) calculate the core of the problem;
b) eliminate or substitute a variable by another one; and
c) redefine the problem using new basic categories.

The algorithm that provides the reduction of conditions can be represented by the following steps:
Step 1: Redefine the value of each attribute according to a certain metric. In this illustrative example, typical ranges in power system operation are used:

- real power values: under 40% of nominal capacity = low (L), between 40% and 60% = medium (M), and above 60 % of nominal capacity = high (H)
- bus voltage values: under 0.95 pu = low (L), between 0.95 and 1.05 = normal (N), and above 1.05 = high (H)
- the status of circuit-breakers are maintained because the values 0 and 1 are normalized already.

Step 2: This next step verifies if any attribute can be eliminated by repetition.
Step 3: This step verifies and eliminates identical examples.
Step 4: This step verifies if the decision table contains only indispensable attributes. This task can be accomplished eliminating step-by-step each attribute and verifying if the table still gives the correct classification. In the example, after considering the elimination of each attribute, B is dispensable for the decision table.

TABLE II
REDUCTION OF THE SET OF EXAMPLES

	Attributes			
U	**A**	**C**	**D**	**S**
1A	0	-	H	L2
1B	-	M	H	L2
2A	1	H	-	L3
2B	1	-	N	L3
2C	-	H	N	L3
3	-	M	L	S
4	-	L	-	L1
5	-	M	N	S
6A	0	H	-	L2
6B	0	-	H	L2
7	1	-	-	L3
8	-	L	-	L1

Step 5: Compute the core of the set of examples. This can be done eliminating each attribute step-by-step, and verifying if the decision table continues to give the correct answer (i.e., it continues to be consistent).

Step 6: This step computes the reduced set of relations that conserve the same inductive classification of the original set of examples. Table 2 contains the reduction of each example.
Step 7: According to Table II, the knowledge existent in Table I can be expressed by the following set of rules:

- If (C is M and D is L) or (C is M and D is N) then S = Safe.
- If C is L then S = Abnormal level 1.
- If (A is 0 and D is H) or (C is M and D is H) or (A is 0 and C is H) then S = Abnormal level 2.
- If (A is 1) or (C is H and D is N) then S = Abnormal level 3.

or, using a *complete rule formulation*:

If (the power flow in transmission line C is between 40% and 60%) and (the voltage on bus D is below 1.05)
then the classification of the current state of the system is safe.

If the power flow in transmission line C is below 40%
then the classification of the current state of the system is unsafe level 1.

If (the voltage on bus D is above 1.05) and (the circuit-breaker A is closed or the power flow in transmission line C is between 40% and 60%)
then the classification of the current state of the system is unsafe level 2.

If (the power flow in transmission line C is above 60%) and (the circuit-breaker A is closed)
then the classification of the current state of the system is unsafe level 2.

If (the circuit-breaker A is opened)
then the classification of the current state of the system is unsafe level 3.

If (the power flow in transmission line C is above 60%) and (the voltage on bus D is between 0.95 and 1.05)
then the classification of the current state of the system is unsafe level 3.

XI. Conclusions

Critical Infrastructures, such Electric Power Systems, are vital for our modern society. Therefore they require protection from a variety of threats and their network is potentially vulnerable to cyber attacks. Intrusion Detection Systems is an important tool to increase the security of such Critical Infrastructures. This paper presents a systematic approach to transform examples in a reduced set of rules for an anomaly detection. This approach uses Rough Set theory and concepts of core and reduction of knowledge. An example for power system control centers has been developed. For the sake of clarity, a reduced database is used in the illustrative example. However, the same methodology is applicable to larger databases. The illustrative example showed that the technique has many advantages, such as simplicity to implementation and good performance.

References

[1] "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets",Washington D.C.,Feb 2003, http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

[2] Gamez, D., Nadjm-Tehrani, S., Bigham, J., Balducelli, C., Burbeck, K., and Chyssler, T., "Chapter 19 Safeguarding Critical Infrastructures", Edited by Professor Hassan B. Diab & Professor Albert Y. Zomaya, "Dependable Computing Systems: Paradigms, Performance Issues, and Applications", Wiley STM, 2000.

[3] Dunn, M., and Wigert, I., "International CIIP Handbook 2004", ETHZ, Zurich, 2004.

[4] "The National Strategy to Secure Cyberspace", Washington D.C.,February,2003,http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

[5] "Homeland Security Act of 2002", Washington D.C., January, 2002, http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf.

[6] IT-Grundschutz Manual 2004, http://www.bsi.bund.de/english/gshb/index.htm.

[7] Falco, J., Stouffer, K., Wavering, A., and Proctor, F., "IT Security for Industrial Control Systems", NISTIR 6859, February 2002.

[8] Oyen, R., "Making Sense of the Myriad of Manufacturing and Control System Security Standards, ISA Expo 2005, Oct., 2005.

[9] Naedele, M., "Standardizing Industrial IT Security – A first Look at the IEC Approach", Emerging Technologies and Factory Automation, 2005, ETFA 2005. 10th IEEE Conference on, Vol. 2, 19-22, Sept. 2005, pp. 857 – 863.

[10] Byres, E. and Lowe, J., "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE 2004 Congress, VDE, Berlin, October, 2004.

[11] Dzung, D., Naedele, M., Von Hoff, T.P., and Crevatin, M., "Security for Industrial Communications Systems", Proceedings of the IEEE, Vol.93, No. 6, June 2005.

[12] Naedele, M., and Dzung, D., "Industrial Information System Security – Part I, Part2, and Part 3", ABB Review 2005.

[13] McHugh, J., Christie, A., and Allen, J., "The role of Intrusion Detection Systems", IEEE Software, September/October/2000.

[14] Hale, J., and Bose, A.,"Information Survivability in the Electric Utility Industry", ISW´98, http://www.cert.org/research/isw/isw98/all_the_papers/no19.html.

[15] Goetz, E., "Cyber Security of the Electric Power Industry", Institute for Security Technology Studies at Dartmouth College", December, 2002 [NERC-CIP,2005] http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.

[16] Oman, P., Schweitzer, E., and Roberts, J., "Protecting the Grid From Cyber Attack, Part II: Safeguarding IEDS, Substations and SCADA Systems", Utility Automation, 7(1), 2002, pp. 25-32.

[17] Axelsson, S., "Intrusion Detection Systems: A Survey and Taxonomy", Chalmers University of Technology, Göteborg, Sweden, March/2000.

[18] McHugh, J., "Intrusion and Intrusion Detection", International Journal of Information Security, Volume 1, Issue 1, Aug 2001, Pages 14 - 35, DOI 10.1007/s102070100001, URL http://dx.doi.org/10.1007/s102070100001.

[19] Bace, R., and Mell, P. "Intrusion Detection Systems", NIST Special Publication on Intrusion Detection System,http://csrc.nist.gov/publication/nistpubs/800-31/sp800-31.pdf.

[20] Lundin, E., and Jonson, E., "Survey of Intrusion Detection Research", Technical Report 02-04, Chalmers University of Technology, Göteborg, Sweeden, 2001.

[21] Mé , L., and Michel, C., "Intrusion Detection: a Bibliograpy," Technical Report SSIR-2001-01, September,2001, SUPELEC, France.

[22] Lunt, T., Tamaru, T., Gilham, F., Jagannathan, R., Neumann, P., Javitz, H., Valdes, A., and Garvey, T., "A Real Time Intrusion Detection Expert System (IDES)", Final Technical Report, Computer Science Lab., SRI International, Menlo Park,, California, Feb., 1992.

[23] Porras, P.A., and Neumann, P.G., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", Proc. National Information Systems Security Confrenece, Baltimore, MD, Oct. 1997.

[24] Forrest, S., Hofmeyer, S.A., Somayaji, A., and Longstaff, T.A., "A Sense of Self for Unix Process", Proc. 1996 IEEE Symp. on Security and Privacy, pp. 120-128, 06-08 May 1996, Oakland,CA.IEEE Computer Security Press, Los Alamitos, CA.

[25] Cansian, A.M., "Desenvolvimento de um Sistema Adaptativo de Detecção de Intrus os em Redes de Computadores", PhD Thesis, Instituto de Física de São Carlos, USP, São Carlos, SP, 1997.

[26] Manikopoulos, C., and Papavassiliou,S., "Network Intrusion and Fault Detection: A Statistical Anomaly Approach", IEEE Communication Magazine, Vol. 40, No. 10, pp. 76-82, Oct 2002.

[27] Fink, G., Ko, C., and Levitt, K., "Automated Detection of Vulnerabilities in privileged Programs by Execution Monitoring", Proc. Of the 10th Annual Computer Security Apps. Conf., pp. 134-144, December 5-9, 1994.

[28] Mukkamala, S., Janoski, G., and Sung, A., "Intrusion Detection Using Neural Networks and Support Vector Machines", IEEE Proceedings, 2002.

[29] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., and Zhou, S., "Specification-based anomaly detection: a new approach for detecting network intrusions", In Proceedings of the 9th ACM Conference on Computer and Communications Security (Washington, DC, USA, November 18 - 22, 2002). V. Atluri, Ed. CCS '02. ACM Press, New York, NY.

[30] Sarasamma, S.T., Qiuming, A., and Huff, J., "Hierarchical Kohonenen Net for Anomaly Detection in Network Security", IEEE Trans. on System, Man, and Cybernetics – Part B, Cybernetics, Vol. 35, No.2, April 2005.

[31] Xiangyang Li, and Nong Ye, "A Supervised Clustering and Classification Algorithm for Mining Data with Mixed Variables", IEEE Trans. On Systems, Man, and Cybernetics, Part a: Systems and Humans, Vol. 36, No. 2, March 2006.

[32] Yu, B., Byres, E., and Howey, C., "Monitoring Controller's "DNA Sequence for System Security", *ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society*, Houston, September 2001.

[33] Martinelli, M., Tronci, E., Dipoppa, E., and Balducelli, C., "Electric Power System Anomaly Detection Using Neural Networks", Lecture Notes in Computer Science, Vol.3213/2004, pp 1242-1248, Springer-Verlag, Heidelberg, Oct. 2004.

[34] Wang, W. and Battiti, R., "Identifying Intrusions in Computer Networks with Principal Component Analysis". Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006), IEEE press society, pp. 270-277, April, 20-22nd, Vienna, Austria.

[35] Song, D., Heywood, M.I., and Zincir-Heywood, A., "Training Genetic Programming on Half a Million Patterns: An Example from Anomaly Detection", IEEE Trans. On Evolutionary Computation, Vol. 9, No. 3, June 2005.

[36] Bigham, J., Gamez, D., and Ning Lu, "Safeguarding SCADA Systems with Anomaly Detection", V.Gorodetsky et al.(Eds.):MMM-ACNS 2003, LNCS 2776, pp. 171-182, Springer-Verlag Berlin Heidelberg, 2003.

[37] Pawlak, Z., "Rough Sets", International Journal of Information and Computer Sciences, Vol.11, pp. 341-356, 1982.

[38] Lambert-Torres, G., "Applications of Rough Sets in Power System Control Center Data Mining", IEEE Power Engineering Society Winter Meeting 2002, Vol. 1, pp. 627-631.

[39] Lambert-Torres, G. et al, "Power System Security Analysis Based on Rough Classification", Rough-Fuzzy Hybridization: New Trend in Decision Making, S.K. Pal & A. Skowron, Springer-Verlag Co., pp. 263-274, 1999.