International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 3444 - 3449

Implementation of Multilayer cybersecurity based on Intrusion Detection System

Mr. Ashish A. Mutha
ME CSE,
PRMIT&R College,
Amravati, India.
ashishmutha10@gmail.com

Prof. Ms. R. R. Tuteja
CSE, Associate professor,
PRMIT&R College,
Amravati, India.
ranu.tuteja@gmail.com

***Abstract*—** Cyber security has become a high priority in Industrial Sector/Automation. Here the dependable operation is to ensure the stable, secure and reliable in power system delivery. By using the Intrusion Detection System framework Obscurity progress can be easily removed. Access control mechanism mainly used to launching the anomalous attacks. This framework provides a hierarchical approach for; integrated security system and comprising distributed IDSs. In a novel SCADA-IDS with whitelists and behavior-based protocol analysis is proposed and it is exemplified in order to detect known and unknown cyber-attacks from inside or outside SCADA systems. Finally, our proposed SCADA-IDS is implemented and it is successfully validated through a series of scenarios performed in a SCADA-specific test bed developed to replicate cyber-attacks against a substation LAN. From the perspective of SCADA system operators, the lack of openly available test dataset is a bottleneck, to compare the performance and accuracy of proposed solutions. However, for the research in the community to progress, such a large dataset would be valuable. The propose system will to creating a new dataset to mitigate vulnerable attack from cyber-crime to save the higher level records and system.

Keywords- *Cybersecurity; intrusion detection; supervisory control and data acquisition (SCADA).*

*****

I. INTRODUCTION

Supervisory control and data-acquisition (SCADA) systems have long played a significant role in power system and become increasingly complex; communication technologies are adopted and interconnected as state-of-the-art information. The increased complexity and interconnection of SCADA systems have exposed them to a wide range of cybersecurity vulnerabilities. Supervisory control and data-acquisition systems with legacy devices lack inbuilt cybersecurity consideration, which has resulted in serious cybersecurity vulnerable points [1]. In practice, unauthorized or malicious access from outside sources, using Internet protocol driven proprietary or local-area networks can threaten SCADA systems by exploiting communication weaknesses to launch simple or elaborate attacks which may lead to denial of service, deliberate maloperation or catastrophic failure, and, consequently, compromise the safety and stability of power system operations [2]. Thus, the requirement to strengthen cybersecurity in SCADA as part of smarter grids is a pertinent priority to ensure reliable operation and govern system stability in terms of communications integrity.

Digital substation environment must be securing is just part of a wider and significant effort that is to be required to ensure the secure operation of advanced power systems delivery [15]. There are two types of IDS in network, network based (NIDS) and host based (HIDS) intrusion detection systems. Thus, some systems may attempt to stop an intrusion or intruder attempt but for the monitoring system it is neither required nor expected. Prevention systems and Intrusion detection are primarily focused on identifying all possible incidents such as logging information about them and also reporting attempts [13]. In addition focused also on organizations which use prevention system and intrusion detection for other purposes, such as detecting individuals from violating security policies, identifying problems with security policies [4] and documenting existing threats.

Monitoring legitimate network traffic or strategies to detect malicious activity on a network can broadly be classed into three areas. These include the analysis of packet content for known signature (referred to as Deep Packet Inspection) [14], the collection of flow based statistical information, and the analysis of network topology or host connection patterns. It must also be scalable to networks of increasing size and must be flexible to allow implementation of the different strategies for traffic analysis. There is a requirement for a tool that can read data from a network in a fast and effective manner [26], allowing real-time analysis.

Network intrusion detection systems (NIDS) are placed at a strategic points within the network and NIDS is used to monitor traffic to and from all devices on the network [26]. NIDS performs an analysis for a passing traffic on the entire subnet, that's work in a promiscuous mode and matches the traffic that is passed on the subnets to the library of known attacks. Once we have identified the attack, abnormal behavior is sensed, and then the alert can be sent to the administrator of system [2]. Example of the network based IDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. Ideally one would scan all outbound and inbound traffic, however doing so might create a bottleneck that would impair the speed of the network overall [19]. The baseline will identify what is normal for that network and what sort of bandwidth is generally used,, what ports, what protocols are used and devices generally connect to each other and alert the administrator or significantly

different, than the baseline or user when traffic is detected which is anomalous. [22] The supervisory control system may be combined with a data acquisition system by adding the use of coded signals over communication channels; to acquire information about the remote equipment status for display or for recording functions.

The enhancement within SCADA connectivity with several advance networks and uses of advance IT infrastructures brought SCADA communication more demandable for end user. SCADA uses centralized station and controller thousand of remote terminal stations at the same time without limitation of networks and protocols. At the other side, highly/many interconnectivity of open standards networks, protocols and uses of open IT infrastructure within SCADA system, made SCADA platform more vulnerable from several types of threads and attacks [22] (Stouffer and Kent, 2006).

With IT technology application, the newly cyber vulnerabilities will emerge in critical infrastructures and similar smart grids. These vulnerabilities could be exploited, not only from outside sources, such as hackers, competitors, terrorists or industrial espionage, but also from inside threats, such as example employees, third-party vendors, or site engineers also. As well as deliberate attacks, cyber vulnerabilities in SCADA systems may also be affected by inadvertent events (e.g. negligence equipment failures, user errors, and natural disasters etc) [25]. Security for protecting the entire smart-grid technology environment requires the consideration of many subsystems that make up the smart grid. For example, distribution-management system, wide-area monitoring protection and control, higher level communication architectures at the grid system level and advanced metering infrastructure. The scope of our system is used to focus on one important sub-system level of the [3] smart-grid environment, specifically cyber-security for digital substations.

II. RELATED WORK

The IDS of rule based system is developed by using data collected by simulate an attacks on IEDs and launching packet smelling attacks using forged address resolution protocol (ARP) packets [18]. The uncovering ability of the system is then tested by simulating attacks and through genuine user activity. Intrusion detection is an effective countermeasure that is yet to be deployed in IEC61850 networks [8]. It's capable of actively countering attacks instead of passive blocking as in a firewall. Compared to a conventional computer network, the threats and countermeasures for an IEC61850 network are different. There-fore, the IDS for IEC61850 has to be developed by using experimental data based upon simulated attacks and packet sniffing [8].

In order to improve the cyber-security of the smart grid by utilizing a hierarchical and distributed intrusion detection system in the wireless mesh network. Security is improved via the classification of intrusion data using AIS algorithms and the Support Vector Machine. The effectiveness of the new model for improving security is demonstrated through multiple simulations [5].

To avoid the cyber-security threats [18], proposes a distributed intrusion detection system for smart grids (SGDIDS) by deploying and developing an intelligent module, analyzing module, in multiple layers of the smart grid. Multiple AMs has been embedded at each level of the smart grid—the home area networks (HANs), wide area networks (WANs) and neighborhood area networks (NANs) is to detect possible cyberattacks and classify malicious data [5].

An approach for the detection of class of cyber-attacks against industrial installations. The key elements of this technique are the concept of Critical State, and the assumption that an attacker aiming at damaging an industrial installation (like a Power Plant), have to modify, for achieving that result, the state of the system from safe to critical. The critical state validation, hardly applicable in traditional ICT systems, finds its natural application in the industrial control field, where the critical states are generally well-known and limited in number. Since the detection is based on the analysis of the system evolution, and not on the analysis of the attack evolution, the IDS, for known critical states, can detect also "zero day attacks" [19]. This paper has been proposed multi-dimensional metric providing a parametric measure of the distance between a given state and the set of critical states. This metric can be used for tracking the evolution of a system, indicating its proximity to the set of predefined critical states [19].

The principal contribution of intelligent intrusion detection system [8] is anomaly detection, and specifically methods based on adaptive learning, can provide a useful intrusion detection capability in process control networks. These techniques were able to detect some basic attacks launched against the MODBUS servers in our DCS test-bed. To evaluate two anomaly detection techniques, namely, pattern-based detection for communication patterns among hosts, and flow-based detection for traffic patterns for individual flows. Pattern based & flow based anomaly detection has proposed here to improve rate of detection.

III. PROPOSED SYSTEM DESIGN

Proposing SCADA-IDS framework for detecting unwanted user on router by extracting information about access control white list, protocol based white list and behavior base rule from the network. The source and destination IDS are all the major attributes going to use in this entire system.
Architecture shows the system architecture of our SCADA IDS system. In the given below Architecture there are operators which are legal users and someone may be attacker. Packets are exchanging through LAN network. There are huge chances of suspicious packets attack into the LAN. Intrusion detection system is fixed into the network as we can see it into the figure.

 ISSN: 2321-8169
3444 - 3449

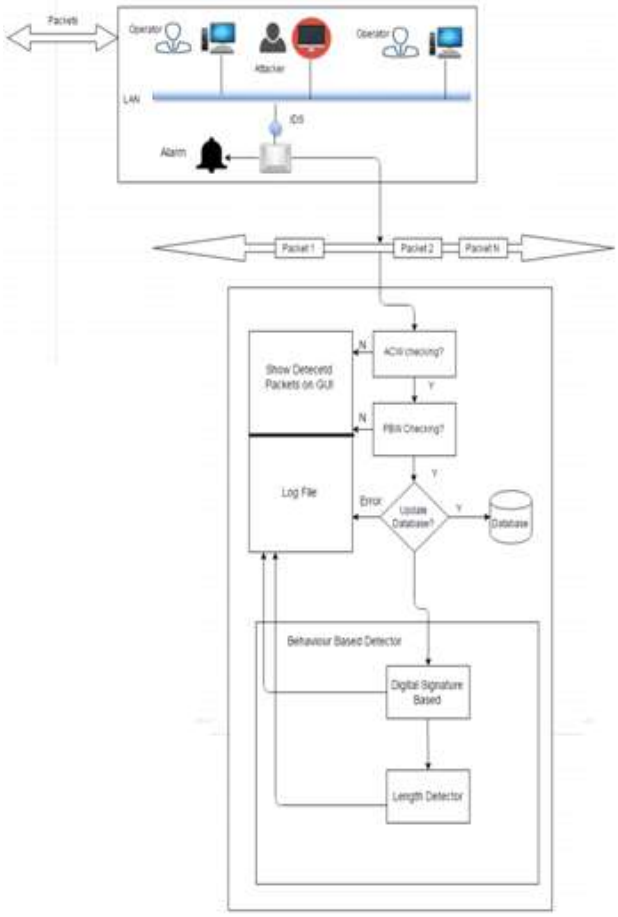

Fig.1 Proposed System Architecture

When packets enter into the network Intrusion Detection System starts its working. Our IDS system is structured of 3 techniques.

1. **ACW (Access Control Whitelist):** In this Intrusion Detection System check whitelist of IP and MAC pair which are present in our LAN system. If corresponding packet doesn't have MAC-IP pair which belongs to whitelist then it will be detected as attack packet. And it will be stored into Log file for future reference. Otherwise packets are not suspicious packets.

2. **PBW (Protocol Based Whitelis**t): If packet belongs to access control whitelist then protocol based whitelist will check that packet. If corresponding packets matches any of the rule which belongs to protocol based whitelist then it will be considered as suspicious packet and it is stored into Log file as well as database.

3. **BBR (Behavior Based Rule):** In this method two techniques are used
   - Digital signature generation: In this method if one operator wants to send any message to another operator which is confidential then for security purpose digital signature method generate keys and signature and sends encrypted data towards receiver. At the receiver end signature will be checked and if it does not match then it is suspicious packet and stored into the log file.
   - Length detector: This method checks length of input packet and the actual payload if it is greater than payload then packet is suspicious and it will be stored into the log file.

When attack found at that time IDS will generate alarm to know about attack detection. In this way whole architecture work and we found the packets are suspicious attack or not.

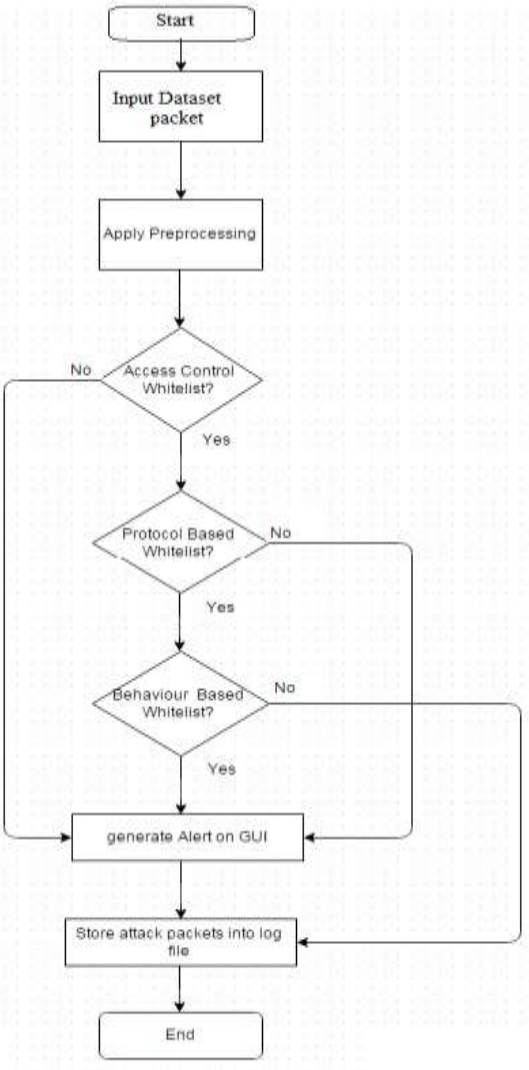

Fig. 2 Flow Execution

IV. SYSTEM IMPLIMENTATION

Mathematical Model

Let S be our proposed system which we use to find the attack detection through ACW, PBW and BBR. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A digital signature technique is developed to enhance and to speed up the process of SCADA.

 ISSN: 2321-8169
3444 - 3449

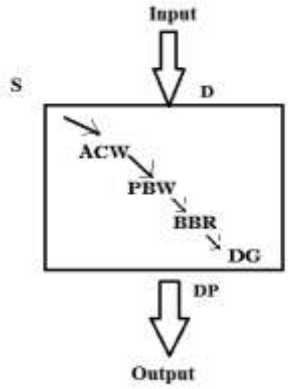

Fig 3. Processes in Detection of Intrusion attacks

S = {D, ACW, PBW, BBW, DP}
Where,
S= System.
D= Dataset.
ACW = Access Control Whitelist.
PBW = Protocol Based Whitelist.
BBW =Behaviour Based Whitelist.
DG= Digital Signature Generation.

Input:

Given arbitrary dataset,

$X = \{x1, x2, \ldots, xn\}$,

Where $xi = [f_1^i, f_2^i, \cdots, f_m^i]T$, $(1 \le i \le n)$ represents the *ith* *m*-dimensional traffic record.

Where x1, x2,…, xn is n number of packets flowing in the network.

ACW (Access Control Whitelist):

$$AC = \{MAC_{src}, MAC_{dst}, IP_{src}, IP_{dst}\}$$

Where MAC_{src} = Source MAC address.
MAC_{dst} = Destination MAC addresses.
IP_{src} = Source IP addresses.
IP_{dst} = Destination IP addresses.

If any of the addresses or ports is not in the corresponding whitelist, the detector will take a predefined action, for example, it will alert in IDS mode and log the detection results. That is

$$AC \notin \{AC_{wl}\} \rightarrow \text{Actions (alert.log)}$$

Where,

$AC = MAC_{src}, MAC_{dst}, IP_{src}, IP_{dst}$ and AC_{wl}

Represent the corresponding whitelist set.

PBW (Protocol Based Whitelist):

Assume there are n number of packets coming from dataset as

D={*x*1, *x*2, …., *xn*},

Where $xi = [f_1^i, f_2^i, \cdots, f_m^i]$ *T*, $(1 \le i \le n)$ represents the *ith* *m*-dimensional traffic record.

R = {r1, r2, … , rn}

Where R is the set of rule for protocol based detection and

r1= Rules of whitelist.

If when the IDS is deployed at the network between two control centers, the protocol-based detector only allows communication traffic complying with specific rules of protocol; otherwise, it will generate an alert message. That is,

$$P \notin \{P_R\} \rightarrow \text{Actions (alert.log)}$$

Where P is the Packet and is Protocol based whitelist which contains rules of detecting intrusion from corresponding traffic.

BBR (Behaviour Based Rules):

Assume there is n number of packets coming from dataset as

D={*x*1, *x*2, · · · , *xn*},

Where $xi = [f_1^i, f_2^i, \cdots, f_m^i]$ *T*, $(1 \le i \le n)$ represents the *ith* *m*-dimensional traffic record.

BBR = {LD, Sig}

Where, BBR is the set of methods for detection of packets belonging to attack packets.
LD=Length Detector
Sig= Signature based Detector.
LD = {P1, P2…Pn}
Where P1,.., Pn are the input packets

When packet contains bytes which indicate the length information about the packet in the payload, it is proposed that a length detector should be applied to detect that whether the number shown in the length bytes is equal to the real length of the payload, such that

$$PL_l \neq PL_{rl} \rightarrow \text{Action (alert, log)}$$

Where PL_l is the length value indicated in the length field of the payload, and PL_{rl} stands for the practical length of the payload. If alert generated then store it into log file.

DG (Digital Signature):

i) Key Generation:

- Choose two large prime numbers p and q and calculate n= p x q
- Calculate $\emptyset(n) = (p-1)x(q-1)$ and Choose e such that gcd $(e, \emptyset(n))=1$

- Calculate d such that $d X e \bmod \emptyset(n) = 1$
- Choose random numbers b and x. Here x should not relative prime to $\emptyset(n)$
- Calculate c such that b^x x c(mod)n=1
- Public key is (n, e, c, x) and private key is (d, b).

ii) Signature Generation:

- Calculate S1 = $H(m)^d \bmod n$
- if x|s1 (i.e. x is a divisor of s1) then generate s1 again.
- Calculate $s2 = (H(m) \times b^{s1}) \bmod n$

H (.) is a one way hash function. (s1, s2) is the signature of message m. Sender sends signature with the message m to receiver.

iii) Signature Verification:

Receiver first calculates H (m) using the received message m and check the following two conditions for signature verification:

- Verify, if $H(m) = s_1^e \bmod n$
- $H(m)^x \equiv s_2^x \times c^{s1} \bmod n$

DP (Detected Packets) :

DP= {n, m}
Where n is normal packets and
M is the malicious packets.

Log (Log File):

Log={x1, x2,.., xn}

Where Log contain the set of detected packets i.e. x1, x2 etc.

If P ACW or PBW or BBR

Where P is the packet if it does not belongs to corresponding whitelist i.e. ACW, PBW and BBR then store that packet into log file.

V. CONCLUSION

The proposed framework is improving the cybersecurity of existing substation computer networks. The SCADA system which combines IDS technology i.e. ACW and PBW and behavioral monitoring to make SCADA systems more secure. This approach is compatible with currently emerging trends to monitor smart grids and other type of critical infrastructure also. In this context, a novel SCADA-IDS with Access control whitelist, Protocol based whitelist and behavior-based analysis is proposed and exemplified in order to detect known and unknown cyber attacks from outside or inside SCADA systems. In our system we implemented the proposed behavior-based algorithm using digital signature technique to monitor the entire sensor network in the network. When attack found IDS will generate signal to know about attack detection. Finally, the proposed SCADA-IDS is implemented and successfully validated through a series of scenarios performed in a SCADA to replicate cyber attacks against a substation LAN system.

REFERENCES

[1] Antiy CERT, "Report on the worm Stuxnet's attack," Harbin, China, Tech rep. V3.1 2010-09.29, Sep. 2011.
[2] A. A. Ghorbani,W. Lu, andM. Tavallaee, *Network Intrusion Detection and Prevention: Concepts and Techniques*. London, U.K.: Springer, 2010, pp. 1–20.
[3] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. SmartGrid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.
[4] J. Verba and M. Milvich, "Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS)," in *Proc. IEEE Conf. Technol. Homeland Security*, 2008, pp. 469–473.
[5] M. P. Coutinho, G. Lambert-Torres, L. E. B. da Silva, H. G.Martins, H. Lazarek, and J. C. Neto, "Anomaly detection in power system control center critical infrastructures using rough classification algorithm," in *Proc. IEEE 3rd Int. Conf.Digital Ecosyst. Technol.*, 2009, pp. 733–738.
[6] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Trans. Ind. Inf.*, vol. 7, no. 2, pp. 179–186, May 2011.
[7] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for SCADA networks," in *Proc. SCADA Security Scientif. Symp.*, 2007, pp. 127–134.
[8] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and T. Jian-Cheng, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010.
[9] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, 2012, pp. 2338–2345.
[10] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.
[11] A. Valdes and S. Cheung, "Communication pattern anomaly detection in process control systems," in *Proc. IEEE Int. Conf. Technol. Homeland Security*, 2009, pp. 22–29.
[12] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. IEEE eCrime Res. Summit*, 2010, pp. 1–9.
[13] E. D. Knapp, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. New York: Elsevier, 2011, pp. 60–61.
[14] J. Hurley, A. Munoz, and S. Sezer, "ITACA: Flexible, scalable network analysis," in *Proc. IEEE Int. Conf. Commun. Ind. Forum Exhibit.*, 2012, pp. 1084–1088.
[15] C. L. Abad and R. I. Bonilla, "An analysis on the schemes for detecting and preventing ARP cache poisoning attacks," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. Workshops*, 2007, p. 60.
[16] Bonnie Zhu, Anthony Joseph, Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems"

Department of EEACS University of California at Berkeley, CA.

[17] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Q. Yao, B. Pranggono, and H. F.Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems," in *Proc. IET Int. Conf. Sustain. Power Gen. Supply*, 2012, pp. 1–8.

[18] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, H.F. Wang," Rule-based intrusion detection system for SCADA networks", the queen's university of Belfast, UK.

[19] E. Egozcue, D. H. Rodríguez, J. A. Ortiz, V. F. Villar, and L. Tarrafeta, "Smart grid security: Recommendations for Europe andmember states. ENISA". Heraklion, Greece., Jul. 2012. [Online]. Available: http:// www.enisa.europa.eu

[20] S. Edgar and A. Burns, "Statistical analysis of WCET for scheduling," in *Proc. IEEE 22nd Real-Time Syst. Symp.*, 2001, pp. 215–224.

[21] I. N. Fovino, A. Carcano, T. De Lacheze Murel, A. Trombetta, and M. Masera, "Modbus/DNP3 state-based intrusion detection system," in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, 2010, pp. 729–736.

[22] A. Shahzad, S. Musa, A. Aborujilah and M. Irfan, "The Security Survey and Analysis on Supervisory Control and Data Acquisition Communication" Science Publications doi:10.3844/jcssp.2014.2006.2019 Published Online 10 (10) 2014.

[23] J. W. Wang and L. L. Rong "Cascade-based attack vulnerability on the US power grid," *Safety Sci.*, vol. 47, no. 10, pp. 1332–1336, Dec.2009.

[24] S. Sen, O. Spatscheck and D. Wang,"Scalable In-Network Identification of P2P Traffic Using Application Signatures", In www2004.

[25] P.Owezarki, J. Mazel and Y. Labit, "0day anomaly detection made possible thanks to machine learning" 8th international conference on wired/wireless Internet communication, WWIC'2010.

[26] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time", USENIX Security.

[27] O. Depren, M. Topallar, E. Anarim and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer network", ES with application, 2005, Vol.29, issue 4, pp.713-722.