Secure Management with SCADA-IDS Framework for Power System Delivery

K. Bharath
PG Scholar, Computer Science and Engineering, Indian Institute of Information Technology, Srirangam, Tiruchirappalli, Tamilnadu, India.

P. Balasubramanian
Faculty, Department of InformationTechnology, Indian Institute of InformationTechnology Srirangam, Tiruchirappalli, Tamilnadu, India.

Abstract – Digital security has turn out to be high need in Industrial Automation (IA).Here reliable operation is to guarantee the safe, steady and dependable in power network delivery. Lack of clarity advancement can be effectively uprooted by utilizing the IDS system. Access control procedure is basically introducing the anomalous attacks. The system gives a progressive way to deal with a coordinated security framework, including distributed IDSs. In this paper, SCADA-IDS with whitelist and behavior-based SCADA proposed and exemplified so as to recognize known and unknown digital attacks from inside or outside SCADA frameworks. At last, the proposed SCADA-IDS is executed and effectively approved through a progression of practical situations performed in a SCADA-specific test bed developed to replicate cyber-attacks against a substation LAN. From the perspective of SCADA system operators, to compare the performance and accuracy of proposed solutions, the lack of openly available test dataset is a bottleneck. However, for research in the community to progress, such a dataset would be valuable. The propose system will to create new dataset to mitigate vulnerable attack from cyber-crime side to save the higher level records and system. Further to improve system performance a hybrid structure of compromised framework with IDS series of realistic situations will be proposed. Digital signature technique has been used to ensure the information which they are going to communicate on each other on networking area. Authenticating value will get sign by sending side and it will re-evaluate by using destination area.

Index Terms – Cyber security; intrusion detection; smart grid; supervisory control and data acquisition (SCADA); Digital signature technique.

1. INTRODUCTION

Supervisory control and data-acquisition (SCADA) systems have long played a significant role in power system operation, becoming increasingly complex and interconnected as state-of-the-art information and communication technologies are adopted. The increased complexity and interconnection of SCADA systems have exposed them to a wide range of cybersecurity vulnerabilities. Furthermore, SCADA systems with legacy devices lack inbuilt cybersecurity consideration, which has resulted in serious cybersecurity vulnerable points. 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. Thus, the requirement to strengthen cybersecurity in SCADA as part of smarter grids, in particular, is a pertinent priority to ensure reliable operation and govern system stability in terms of communications integrity.

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) [1], the collection of flow based statistical information, and the analysis of network topology or host connection patterns. However, the specifics of these approaches and their implementations can vary greatly. There is a requirement for a tool that can read data from a network in a fast and effective manner, allowing real-time analysis. It must also be scalable to networks of increasing size and must be flexible to allow implementation of the different strategies for traffic analysis.
A power grid can become vulnerable with respect to electronic intrusions that are launched to manipulate critical cyber assets for the purpose of a cyber-attack. The complexity of cascading events triggered through the substation level control systems can de-energize power system components and aggravate operating conditions by causing overloading and instability. An analytical method system has been used to model the attack upon substations that may initiate cascading failures. Cybersecurity of intelligent electronic devices in the substations has been recognized as a critical issue for the smart grid[15]. One way to address these issues is to develop new technologies to detect and disrupt malicious activities across the networks. Anomaly detection system is an early warning mechanism to extract relevant cybersecurity events from substations and correlate these events. Some reports described penetration testing conducted by private companies

to try to connect from an external network to internal critical cyber assets, e.g., programmable electronic devices and communication networks. It is shown that cyber assets are accessible from remote access points, e.g., modem over a landline, wireless technology, or virtual private network (VPN) using a routable. This concerned with the sources of vulnerabilities due to cyber-intrusions at the substations of a power grid. Trust-based security mechanisms have been designed to suppress cyber-attacks or other malicious events for event logging, analysis, or blocking power system operations . Data objects for intrusion detection are categorized in the IEC 62351[3].

Modern control systems are machine based structures that screen and control techniques that exist in the physical world. Current security countermeasures in SCADA[2] frameworks chiefly concentrate on securing frameworks from outside interruptions or malevolent assaults. Case in point, approaching activity to substations, control focuses, and corporate systems will be reviewed by business firewalls or IDS. On the other hand, this security approach just considers border resistances and disregards inside identification inside a substation system or a control focus. For in-stance, an architect can enter a substation and join his or her portable computer to the LAN.

The enhancement within SCADA connectivity with several advance networks and uses of advance IT infrastructures brought SCADA communication more demandable for end user. The scope of this system is to focus on some important sub-system level of the whitelist based environment, specifically cyber-security for digital substations. So the main objective of our system is to implement goals which we proposed and to secure the SCADA system from various suspicious attacks.

2. RELATED WORK

SCADA systems are used to control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society. The security of these SCADA systems is important because compromise or destruction of these systems would impact multiple areas of society far removed from the original compromise. For example, a blackout caused by a compromised electrical SCADA system would cause financial losses to all the customers that received electricity from that source. How security will affect legacy SCADA and new deployments remains to be seen.

An intrusion is an activity or a sequence of activities that result in a compromise or intend to compromise the aspects of information assurance. Intrusion detection is a security technology of great significance to critical infrastructure protection that attempts to detect, and respond to intrusions against information and information systems. IDSs that rely on audit trails for deciding whether a particular activity is intrusive or not; compliments other security technologies (firewalls, file integrity checkers, vulnerability scanners, and antivirus tools). IDS also provide information for forensic analysis and to detect non-repudiation activities based on the audit trails collected. IDS that detect intrusions based on deviations from normal to abnormal state using user or systems profiles is defined as anomaly detection. Anomaly detection tends to detect novel attacks with the expense of false positives. Signatures are a set of actions, conditions or activities, when met indicate an intrusion. IDS that rely on signatures are defined as misuse or signature based detection systems. Misuse detection systems tend to higher detection rate with the expense of false negatives.

IDSs have been introduced with SCADA frameworks utilizing factual ways to deal with arrange system movement as typical or irregular. To build the statistical models, different demonstrating routines can be utilized, for example, neural systems, regression models, and Bayesian systems [2]. In any case, generally measurable interruption systems create false positives which bring about false alarms, and false negatives which miss genuine assaults.

The IDS of this paper is developed by using data collected by simulate an attacks on IEDs and launching packet smelling attacks using forged address resolution protocol (ARP) packets. 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 [3]. 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 [3].

Keeping in mind the end goal to enhance the digital security of the shrewd lattice by using a various leveled and circulated interruption location framework in the remote cross section system. Security is enhanced through the characterization of interruption information utilizing the SVM and AIS algorithms. The adequacy of the new model for enhancing security is shown through different reenactments [3].

A system for the revelation of class of advanced attacks against mechanical foundations. The key segments of this system are the way to go of Critical State, and the assumption that an attacker going for hurting a mechanical foundation (like a Power Plant),have to change, for finishing that come to fruition, the condition of the structure from ensured to fundamental. The segregating state endorsement, hardly material in traditional ICT structures, feels that its standard application in the mechanical control field, where the fundamental states are overall surely understood and limited

in number. Since the disclosure is concentrated around the examination of the system improvement, and not on the analyzation of the attack progression, the IDS, for known separating states, can recognize similarly "zero day attacks." [4]. The paper has proposed multi-dimensional metric giving a parametric measure of the partition between a given state and the arrangement of separating states. This metric can be used for taking after the improvement of a system, demonstrating its proximity to the arrangement of predefined separating states [4].

The primary commitment of this paper [5] is a show that peculiarity recognition, and particularly techniques in view of versatile learning, can give a helpful interruption identification ability in procedure control systems. To assess two irregularity discovery methods, to be specific, pattern-based detection for correspondence designs among hosts, and flow-based detection for traffic patterns for individual flow. These systems had the capacity distinguish some essential attacks dispatched against the MODBUS servers in our DCS proving ground. Pattern based & flow based anomaly detection has proposed here to enhance rate of detection.

3. PORPOSED MODELLING

Proposing SCADA-IDS framework for detecting unwanted user on router, by extracting information about access control white list,

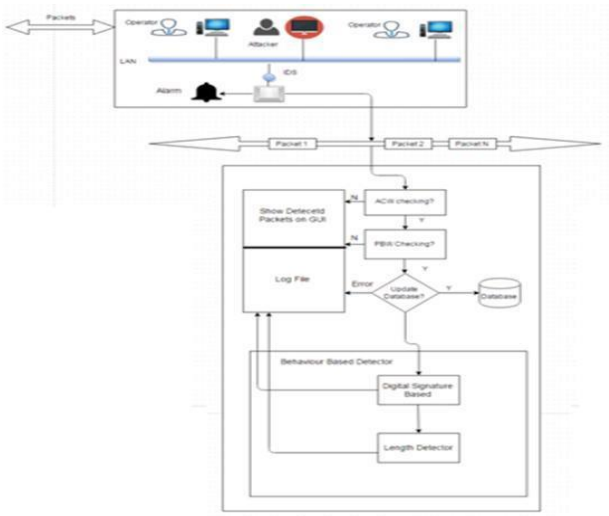

Fig.1Proposed System Architecture

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 our entire system.

Above Architecture shows the system architecture of our SCADA IDS system. In the given above 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.

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

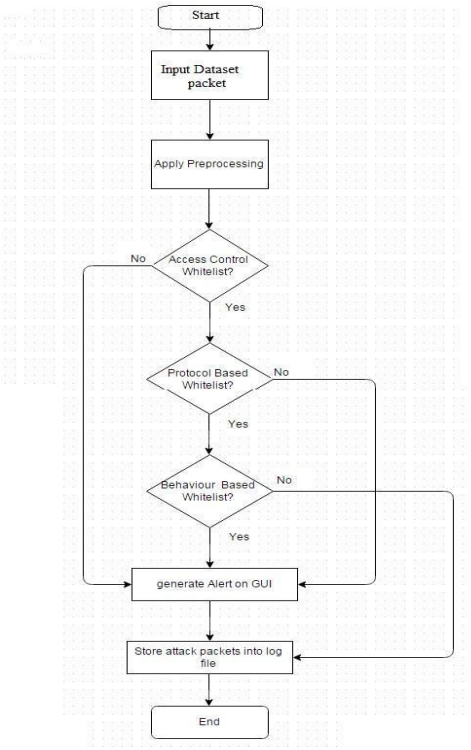

Fig.2 Flow Execution

3.1 ACW (Access Control Whitelist): In this IDS check whitelist of MAC and IP pair which are present in our LAN. If corresponding packet does not have MAC-IP pair which belongs to whitelist then it will be detected as attack packet and which will be stored into Log file for future reference. Otherwise packets are not suspicious packets.

3.2 PBW (Protocol Based Whitelist): If packet belongs to 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 stored into Log file as well as database.

3.3 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 the actual payload and length of input packet if it is greater than payload then

packet is suspicious and 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.

Process Flow of system is started then we giving the input packets to the system from the dataset. After that we are applying the preprocessing because there are many repeated packets in the network so applying preprocessing reduces the process time packets. Next, there is Access Control whitelists it will checks all MAC and IP pair in the predefined whitelist if there is match found then packets are valid packets otherwise packets are suspicious packets or attack and it generate alert on GUI. After that Protocol Based whitelist, it will check all packets with predefined rules if any of rule match then it is suspicious attack or packets, it will generate alert on GUI and otherwise it is valid packet. After that Behaviour Based whitelist, it contains digital signature and length detector. Digital Signature generates key and signature and at the receiver side it will match that signature. If it matches then its valid packets otherwise it is suspicious attack. In length detector it will check actual payload and length of packets if payload length is greater than length of packets then it is suspicious attack or packet. All the attacks packets are store into the log file for the further use.

4. PROPOSED ALGORITHAM

Let S be the proposed system which we use to find the attack detection system through ACW, PBW, BBR and digital signature generation. 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.

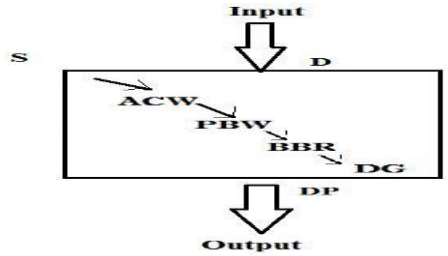

Fig 3. Processes in Detection of Intrusion attacks.

As we can see in Fig 1.
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 an arbitrary dataset X = {x1, x2,….,xn},

Where xi =[…….]T , (1 ≤ i ≤ n) represents the ith m-dimensiona

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

4.1 ACW (Access Control Whitelist).

= Destination IP address.

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.

4.2 PBW(Protocol Based Whitelist)

Assume there are n packets coming from dataset as
D={x1, x2, ….,xn},

R={r1,r2,....m}
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. Where P is the Packet and is Protocol based whitelist which contains rules of detecting intrusion from corresponding traffic.

4.3 BBR(Behaviour Based Rules)

Assume there are n packets coming from
dataset as D={x1,x2,.....xn}
{T, (<_=i<=n)represents the i th m-dimensional traffic record}
BBR={L,D,Sig}
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.
If alert generated then store it into log file

4.4 DG (Digital Signature):

i) Key Generation:

Choose two large prime numbers p and q and
calculate n= p xq
- Public key is (n, e, c, x) and private key is (d, b).

ii) Signature Generation:

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.

4.5 DP (Detected Packets):

Where n is normal packets and M is the malicious packets.

Log (Log File):
Log={x1, x2,..,xn}

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.

5. SIMULATION RESULT

Detecting attackers has been primarily compare among three algorithms, attackers detection precision can be assure this parameter.
We have defined the graph through calculating recall and precision values.

$$\text{recall} = \frac{|\{\text{relevant documents}\} \cap \{\text{retrieved documents}\}|}{|\{\text{relevant documents}\}|}$$

Recall in information retrieval is the fraction of the documents that are relevant to the query that are successfully retrieved.

Precision is the probability that a (randomly selected) retrieved document is relevant. Precision and recall are then defined as:

$$\text{Precision} = \frac{tp}{tp + fp}$$
$$\text{Recall} = \frac{tp}{tp + fn}$$

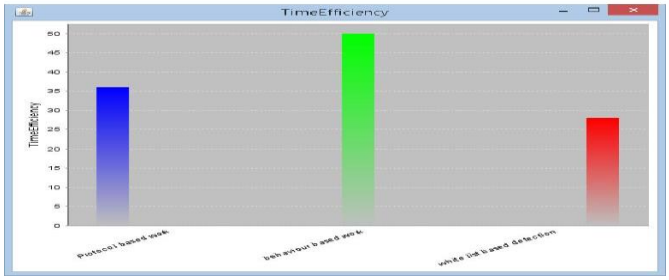

Fig 4.Time Efficiency.

6. CONCLUSION

The proposed framework is intended to improve the cybersecurity of existing substation computer networks. The SCADA system which combines IDS technology and behavioral monitoring to make SCADA systems more secure. This approach is compatible with currently emerging trends to monitor smart grids and other critical infrastructure. 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 inside or outside SCADA systems. In our system we implemented the proposed behavior-based algorithm using digital signature technique to monitor the entire sensor 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 realistic scenarios performed in a SCADA to replicate cyber attacks against a substation LAN.

REFERENCES

[1] A.A.Ghorbani, W.Lu, and M.Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques. 2010, pp. 1–20.

[2] Y. Yang, K. McLaughlin, S. Sezer, ,T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks" IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 29, NO. 3, JUNE 2014, pp. 1092-1102

[3] UpekaKanchanaPremaratne, JagathSamarabandu ,"An Intrusion Detection System for IEC61850 Automated" IEEE TRANSACTIONS
ON POWER DELIVERY, VOL. 25, NO. 4, OCTOBER 2010,pp2376-2383

[4] A.Carcano,A. Coletta,M.Guglielmi,M. Masera "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems"
IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 2, MAY 2011 ppt 179-186.

[5] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for MODBUSRTU and ASCII industrial control systems,"inProc.,2012,pp.2338–2345

[6] Z. Trabelsi and K. Shuaib, "Man in the middle intrusion detection," in Proc. IEEE Global Telecommun. Conf., 2006, pp. 1–6.

[7] E. D. Knapp, Industrial Network Security: Securing Critical Infra-structure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2011, pp. 60–61.

[8] J. Hurley, A. Munoz, and S. Sezer, "ITACA: Flexible, scalable net-work analysis," in 2012, pp. 1084–1088.

[9] IBM, "IBM security QRadar SIEM," Somers, NY, USA, Tech. rep.WGD03021-USEN-00, Jan. 2013.

[10] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smartgrids," vol.2,no.4,pp.796–808, Dec. 2011.

[11] M. Crosbie and G. Spafford, "Applying genetic programming to ntrusion detection," presented at the AAAI Fall Symp. Series, AAAI Press, MenloPark, CA, Tech. Rep. FS-95-01, 1995

[12] W. Lu and I. Traore, "Detecting new forms of network intrusion using genetic programming,"Comput. Intell., vol. 20, no. 3, pp. 474–494,2004.

[13] "Communication Pattern Anomaly Detection In Process Control Systems" Alfonso Valdes, Steven Cheung 22 - 29 11-12 May 2009 978-1-4244-4178-5

[14] P. Gross, J. Parekh, and G. Kaiser, "Secure selecticast for collaborative intrusion detection systems," inProc. Int. Workshop on DEBS, 2004

[15] 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 inves-tigating cyber-security vulnerabilities in smart grid SCADA systems,"inProc. IET Int. Conf. Sustain. Power Gen. Supply, 2012, pp. 1–8.

[16] IEEE Standard Communication Delivery Time Performance Require-ments for Electric Power Substation Automation, IEEE Standard 1646–2004, Feb. 2005.

[17] De Ocampo, Frances Bernadette C, Del Castillo, Trisha Mari L Gomez, Miguel Alberto N "AUTOMATED SIGNATURE CREATOR FOR A SIGNATURE BASED INTRUSION DETECTION SYSTEM WITH NETWORK ATTACK DETECTION CAPABILITIES (PANCAKES)" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 25-35 , 2013 (ISSN: 2305-0012)

[18] Huang Lu, Jie Li, and Hisao Kameda "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature"This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceeding.