International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.6., 2015
(Nov.-Dec.,)

RESEARCH ARTICLE

ISSN: 2321-7758

SECURE AND ATTACKERS AVOIDED SYSTEM FOR SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

K.BHARATH[1], P.BALASUBRAMANIAN[2]

[1]PG Scholar, Computer Science ,Indian Institute of Information Technology,Srirangam , Tiruchirappalli, Tamil Nadu.

[2]Faculty, Department of Information Technology, Indian Institute of InformationTechnology, Srirangam , Tiruchirappalli, Tamil Nadu

ABSTRACT

Consistency and connectivity to the Internet, managerial Control and Data Acquisition systems (SCADA) at the present countenance the risk of cyber attacks. SCADA systems be considered devoid of cyber security in mind and hence the problem of how to adjust conservative Information Technology (IT) interruption detection techniques to suit the wants of SCADA is a big challenge. Explain the nuance associated with the job of SCADA-septic interruption detection and structure it in the domain attention of control engineers and researchers to illuminate the difficulty space. This system mainly proposes a direct admin monitoring alert system is used to find the attackers with the help of a multilayer cyber-security framework based on IDS for protecting SCADA cyber security in smart grids without compromising the availability of normal data. The future system creates new datasets to mitigate defenseless attacks from cyber-crime face to save the senior level records and system. The simulation consequence shows that performance based technique outperforms the additional two methods with respect to time competence and accuracy.

Keywords: Cyber security; intrusion detection; smart grid; supervisory control and data acquisition (SCADA); digital signature technique.

I. INTRODUCTION

Present safety countermeasures in SCADA (supervisory control and data acquisition) frameworks mainly think on ensuring frameworks as of external interruption or spiteful assault. For example, future movement to substations manages focuses, and company systems investigated by business firewalls or IDS. However, this safety move toward just consider border safeguard and overlooks internal part position within a substation system or a manage focus. For instance, a designer can enter a substation and associate his or her smart phone to the local area network (LAN). A focused or unintentional physical attack by means of an impure smart handset at the present have an improved shot of achievement in light of the fact that border resistances have been avoid. In perform and in most detrimental opportunity situation, the greater part of the digital holdings in SCADA frameworks ought to be viewed as unprotected. Be that as it may, incapable to require that all cyber resources meet the majority noteworthy safety requirements

because of budgetary charge, time and framework necessities.

Manufacturing manage frameworks are device based frameworks that monitor and manage contemporary methodologies that be in the physical world. Present safety countermeasures in SCADA frameworks mostly give attention to on securing frameworks from exterior interruption or malicious attacks. Case in point, imminent activity to substations, control focuses, and commercial systems reviewed by business firewalls or IDS. On the other hand, this security move toward just considers border resistances and disregards inside recognition inside a substation system or a manage focus. There-fore, a designer can enter a substation and adhere his or her portable computer to the LAN. With the application of IT innovations, new digital vulnerabilities expand in keen lattices and relative basic bases. These vulnerabilities could be tainted, not just from faint sources, for example, terrorists, programmers, contenders, or perfunctory scrutiny, additionally from inside dangers, for example, ex-workers, displeased representatives, outsider merchants, or site engineers. Safety for defensive the whole smart-grid techno-logical atmosphere requires the thought of many subsystems that make up the smart grid, for example, wide-area monitoring protection and control (WAMPAC), distribution-management system (DMS), advanced metering infrastructure (AMI), and higher level communication architectures at the grid system level. The range of this paper is to focus on one important subsystem level of the smart grid environment, specifically cyber-security for digital substations.

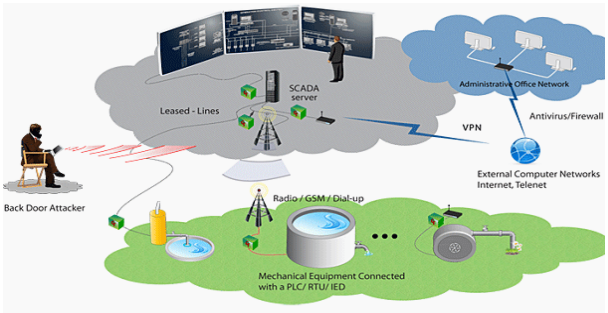

Fig 1: Supervisory Control and Data Acquisition (SCADA) Systems

II. RELATED WORK

This paper describes a place of 28 cyber attacks next to manufacturing control system which employ the MODBUS request layer network procedure. The paper also describes a set of separate and condition based interruption discovery scheme rules which be able to be used to notice cyber attacks and to store proof of attacks for post incident analysis. All attacks described in this paper were validated in laboratory surroundings. The discovery speed of the interruption discovery scheme system obtainable by attack group is also obtainable.

Implementing a additional Specific and additional intelligent packet check up mechanism, modified traffic flow investigation, and sole packet tampering discovery, IDS technology developed particularly for SCADA environment can be deployed with self-assurance in detecting Malicious movement Jared Verba [4]**.** Notice suspect or malicious packets, but is incomplete by the signatures distinct. Present IDS technologies have a possibility at detecting irregular movement (network scans, malformed packets, operating system-level attacks), but the be short of verification in the SCADA environment income there is not anything to stop an attacker as of forging genuine and right instructions or data feed. Lingfeng Wang [1] This technique is able to be used to mystify a system or leave it in a dangerous state without employ those attack technique that IT-driven IDSs be developed to notice.

A learning-based move toward or detect irregular network traffic pattern. This irregular pattern might communicate to attack behavior such as malware spread or refutation of service. Alfonso Valdes [6] Misuse discovery, the normal intrusion discovery move toward used today, characteristically use attack signatures to notice known, exact attacks, but may not be capable against new or variation of recognized attacks. Our move toward, which does not rely on attack-specific information, may provide balancing discovery ability for protecting digital manages systems.

The major focus of the paper is on man-in-the-middle attacks, covering alteration and

inoculation of instructions, it also particulars imprison and play again attacks. Peter Maynard [11] A first set of attacks are performed on a restricted software simulated laboratory. Last experiments and corroboration of a man-in-the-middle attack are performing in a complete tested surroundings in combination with an electrical energy sharing worker.

III. MULTIATTRIBUTE SCADA SPECIFIC INTRUSION DETECTION SYSTEM FOR POWER NETWORKS

This paper has obtainable a covered cyber safety structure for SCADA systems which combine safety enclaves, IDS technology, and behavioral checking to create SCADA systems additional safe. The structure provides a hierarchical move toward for an integrated safety scheme, comprising dispersed IDSs. This move toward is well-matched with at present up-and-coming trends toward using SIEM technology to check.

Smart grids and other dangerous communications. In this context, novel SCADA-IDS with white lists and behavior-based SCADA protocol psychoanalysis is future and exemplified in arrange to notice known and unknown cyber attacks from inside or outside SCADA systems. Fatly, the futures SCADA-IDS is implemented and productively validate through a series of realistic scenarios perform in a SCADA-specific tested urbanized to duplicate cyber attacks against a substation LAN. Digital substations are dangerous nodes that are essential to the core function of electrical energy grids. as a result, their reliable operation is essential to ensure that power release leftovers secure, stable, and reliable.

In the background of the rapid growth and deployment of digital substations approximately the world, opportune investigate on up-and-coming cyber safety issues in this area is an extremely pertinent and urgent issue.

Though, securing the digital substation surroundings is just fraction of a wider and significiently attempt that is necessary to make sure the safe process of higher power systems.

A lot of challenge remains to be address in additional subsystems and for the senior level communications structural design where subsystems are consistent.

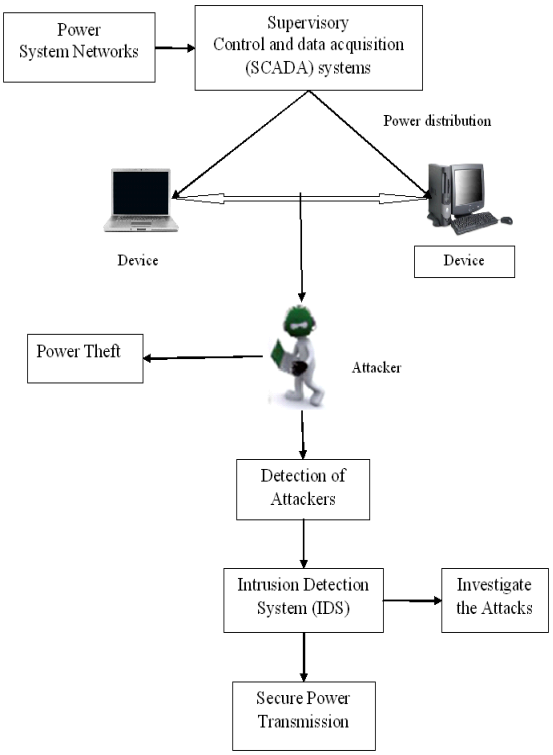

Fig 2: Multiattribute SCADA Specific Intrusion Detection System for Power Networks

IV. PROPOSED METHODOLOGY

MULTIATTRIBUTE IDS FOR SCADA

In comparison with traditional IT networks, SCADA systems have distinguishing features, such as the use of a limited number of packets (low throughput), a fixed number of Communication devices, a limited number of communication protocols, and regular communication and behavior patterns. Therefore, a SCADA-specific IDS is proposed as an effective tool to identify external malicious attacks and internal unintended misuse. The proposed hybrid intrusion detection method consists of three attributes: 1) access-control white list; 2) protocol- based white lists; and 3) behavior-based rules

ACCESS-CONTROL WHITE LISTS (ACWS)

The access-control white list approach contains detectors in three layers, that is, source and destination medium-access control addresses in the Ethernet layer, source, and destination IP addresses in the network layer, and source and destination

portsmin the transport layer. If any of the addresses or ports is not in the corresponding white list, the detector will take a predefined action, for example, it will alert in IDS mode and log the detection results. That is In addition, each host or device in a SCADA system has a unique match. If the device has not been replaced with new hardware and the same IP address of the device is detected from two or more MAC addresses, it means that a spoofing attack may be taking place.

PROTOCOL-BASED WHITELISTS (PBWS)

The aforementioned access-control white list refers to layers in terms of the open systems interconnection (OSI) model. The protocol-based white list method is related to the application layer (up to layer 7) and deals with various SCADA protocols, such as Mod bus, DNP3, IEC 60870-5 series, ICCP, IEC 61850, and proprietary protocols. In different scenarios, the detector can be set to support specific protocols. For example, when the IDS is deployed at the network between two control centers, the protocol-based detector only allows communication traffic Complying with specific protocols; otherwise, it will generate an alert message.

BEHAVIOR-BASED RULES (BBRS)

As a necessary complement to the aforementioned white list methods, a behavior-based detection approach finds and definesnormal and correct behaviors by deep packet inspection (DPI).This may include the analysis of a single packet or multiplepacket together. SCADA-IDS in different scenarios may havedifferent rules in terms of normal behaviors. If the IDS is locatedbetween an HMI and a protocol gateway within a substation, several behavior-based detectors are proposed and defined as follows.

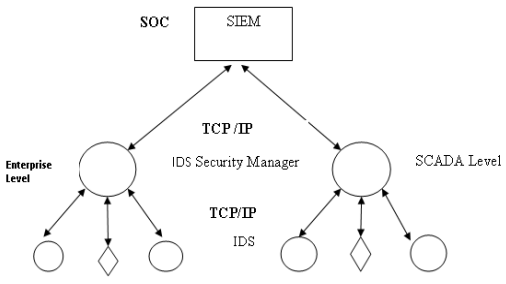

Fig 3: Framework

V. EXPERIMENTAL RESULTS

The white lists-based, protocol-based and behavior-based method studied & implemented the intrusion detection techniques; the behavior based algorithm method with digital signature technique is proposed in order to monitor the entire sensor network. Also based on the Simulation results. It reflects that the performance is improved in terms of accuracy & time efficiency with the help of Behavior Based Technique as compared with Access Control White list & Protocol Based techniques. Thus proposed Technique helps in better monitoring of cybercrime process in networking.

VI. CONCLUSION

The framework provides a hierarchical approach for an integrated security system, comprising distributed IDSs. This approach is compatible with currently emerging trends toward using SIEM technology to monitor smart grids and other critical infrastructure. In this context, a novel SCADA-IDS with white lists and behavior-based SCADA protocol analysis is proposed and exemplified in order to detect known and unknown cyber attacks from inside or outside SCADA systems. Finally, the proposed SCADA-IDS is implemented and successfully validated through a series of realistic scenarios performed in a SCADA-specific test bed developed to replicate cyber attacks against a substation LAN. Both model-based intrusion detection and middleware-level intrusion detection build models to specify the normal behavior of the network traffic and compare the SCADA traffic against these models to detect potential anomalous behavior. Model-based detection is an important complement to signature-based approaches. The specification-based IDS have an inviting advantage to SCADA systems and networked control systems in general.

REFERENCES:

[1]. Y. Yang, K. McLaughlin, S. Sezer, Member, IEEE, T. Littler, E. G. Im, Member, IEEE, B. Pranggono, Member, IEEE, and H. F. Wang, Senior Member, IEEE

[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]. 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.

[7]. 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.

[8]. 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.

[9]. C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cyber security of the substations," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[10]. 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.

[11]. 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. 18