International Journal of Trend in Research and Development, Volume 2(6), ISSN: 2394-9333
www.ijtrd.com

Anomaly Detection for Cyber Security of the Substations: A Survey

[1]K.Krishneswari, [2]N.Jayasri,
[1]PhD, Head of Computer Science Department, [2]ME,
Department of Computer Science and Engineering, Tamilnadu College of Engineering,
Coimbatore, India.

Abstract: Smart Grid the enhancement of power grid presents undetermined level of risk to power grid reliability.It is an evolution of current electrical grid.The source of vulnerability of a power grid is the cyber intrusions as most substations are unmanned and low protection in physical security. Cyber security technologies for anomaly based detection at a substation arein an early stage of development. Technologies are to be developed which are critically needed to detect anomalies for substation automation multicast protocols and applications in network. Intrusion detection is the process of detecting the hacker.In this paper, wepresents a review on various IDS (Intrusion Detection System) used in anomaly detection for cyber security of substations in power grid and a comprehensive survey ofcyber security issues for the Smart Grid substations.

Keywords: *IDS, Cyber Security of Substations, GOOSE , SMV Anomaly Detection ,Modbus, DNP3, IEC 60807,IEC 61850, IEC 62351*

I. INTRODUCTION

Smart Grid, the next-generation of power system is considered as a revolutionary and evolutionary regime of existing power grids. The silent features along with Smart Grid is cyber security, which emerges to be a critical issues as millions of electronic devices in the network are inter-connected throughout critical power facilities, that relays based on the immediate impact on reliabilityof widespread infrastructure[4,5]. Securing the advancedsubstation environment is an important process and is simply piece of a more extensive and significant exertion that is obliged to guarantee the safe operation. On the increase of deploying information and communication technology(ICT), incorporating cyber intrusion is an important threat smart grid which organize cyber attacks at various substations may activate a sequence of that leads to collapse[1,2]. Figure 1 shows the network architecture in smart grid.

Substation automation on IEC 61850 is a key element to achieve interoperability in smart grid[3].IEC 61850 modelsprovide rules for organizing data in such a manner that it is consistent across all types of electronic Intelligent Electronic Devices (IEDs). Generic Object Oriented Substation Events (GOOSE) and SMV messages form part of the IEC 61850 protocol, which are network based on network based anomaly detection is embedded selected logical and analog data are transmitted in Ethernet packets [10].In this paper we present a review on attacks in protocol and then survey about network based anomaly protocols, DNP3, IEC 60807, IEC 61850, IEC 62351 and the security issues for smart grid substations.

Figure 1: The Network Architecture In The Smart Grid: Backbone and Local-Area Networks.

II. LITERATURE REVIEW

A. Basic Attacks on Communications

Basic attacks on communications are Dos(Denial of service) attack which will appear in all the layers of OSI model. This attack makes the service being unavailable temporarily. Physical security of widely dispersed communication infrastructure is often not possible but in wired cellular communications can be jammed to prevent communication [6]. ARP (Address Resolution protocol) spoofing and MAC flooding will be appeared on network layer and data link layer. It gather data or as first step towards more attacks, such as Man-In- The – Middle, Session hijacking [7]. MITM attack which acts as a trusted node and communicates between the two nodes, it drops the packets[8]. Reply attack, session hijacking, Injection [9] and miscellaneous attacks are the other attacks in communication network.

III. COMMUNICATION PROTOCOLS

A. MODBUS [11, 12, 13]

Modbus is an application layer messaging protocol, positioned at level 7 of the OSI model, whichprovides client/server communication between devices connected on different types of buses ornetworks. The industry s serial de facto standard since 1979, truly open and the most widely

usednetwork protocol in the industrial manufacturing environment. The Modbus protocol provides anindustry standard method that Modbus devices use for parsing messages.The Internet community can access Modbus at a reserved system port 502 on theTCP/IP stack. Modbus is used to monitor and program devices; to communicate intelligentdevices with sensors and instruments; to monitor field devices using PCs and HMIs [13].

B. DNP3

DNP3 is extensively-used for both intra and inter substationcommunications in US powersystems[13]. It was designed to transfer message without anysecurity mechanism. Since it is not very practical to upgradeall legacy DNP3-based power systems into new onesin 1 day, it is essential to modify or even overhaul DNP3 toadopt more security functionalities to make a large numberof legacy power devices keep pace with securityrequirements in the Smart Grid.Researchers [14, 15, and 16]have already started to designsecurity functionalities for DNP3 based on two main solutions:(1) modify the original protocol to introduce securitymechanisms to the DNP3 stack and (2) insert a securitylayer between the TCP/IP layer and the DNP3 protocolstack. The former will provide the security suits only forDNP3 regardless of the lower layer configuration;however,it needs tedious modification of the protocol stack and requiresthe upgrade of communication systems in powerdevices. The latterdoes not need tochange any of the DNP3 protocol stack. It enables legacy systems to communicate with the Smart Grid via protocol translation devices.From the above description, it is clear that inserting asecurity layer between DNP3 and TCP/IP is more desirableto make legacy devices compatible with smart gird devices.Specifically, the objective of this security layer is to helpthe DNP3 protocol achieve basic security requirementsfor integrity and confidentiality. At the transmitter, thesecurity layer intercepts DNP3 packets distributed to theTCP/IP layer, encrypts the data, then sends encrypted packetsinto the TCP/IP layer. At the receiver, the security layerdecrypts data packets from the TCP/IP layer, and passesthem to the application layer (DNP3 layers). Either symmetricor asymmetric algorithms can be used to provideprotection of integrity and confidentiality for DNP3 packets.For example, MAC-based authentication is designedand implemented in [16]as a security extension toDNP3-based communication for distribution automationsystems.

C. IEC 61850 and IEC 62351

IEC 61850 and IEC 62351IEC 61850, a recent standard for substation communication,comes without its own security mechanisms. Thesecurity of IEC 61850 relies on IEC 62351 [17], which isa standard proposed to handle the security for a series ofprotocols including IEC 61850. In the following, we brieflydiscuss how IEC 62351 enforces security for IEC 61850.IEC 62351 defines both authentication and encryptionmechanisms for IEC 61850 communication.

1. An authentication and encryption layer above the TCP/IP layer. This layer enforces TLS to use symmetric cryptographyand MACs for message confidentiality and authenticity. This layer is intentionally used for lesstime-critical messages based on TCP/IP in substationsystems.

2. An authentication layer between the MAC and IP layers. This layer is specifically used for authenticating timecriticalmessages in IEC 61850 that do not pass throughthe TCP/IP layer, i.e., GOOSE and SMV. To ensure thatsuch messages can be delivered in a timely manner,IEC 62351 defines no data encryption mechanism forthis layer, thus time-critical messages in IEC 61850
are only protected for authenticity.

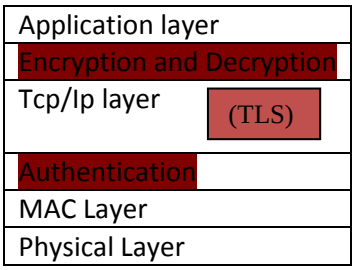

Figure 2: IEC 1850 with IEC 62351

Compared with secure DNP3, Modbus, IEC 61850 with IEC 62351is a modern power communication protocol that balancesthe tradeoff between security and time-criticality by usingtwo distinct security layers for different message types inpower systems. It can be expected that more comprehensivesecurity layering mechanisms will be proposed toachieve both security and QoS requirements for message delivery in the Smart Grid.

IV. SECURE DATA AGGREGATION PROTOCOLS WITH INTEGRATED ANOMALY DETECTION:

Secure DNP3 and IEC 61850 with IEC 62351 are proposed to achieve end-to-end security for power grid communications.Besides such end-to-end security protocols, secure data aggregation protocols are also proposed for the Smart Grid [18,19], since the bottom-up traffic model (device-to-center) is pervasive in power systems, such as metering reading in the AMI network and device monitoring in the SCADA network. In such a communication model, data aggregation protocols with in-network data processing will be more efficient than end-to-end routingprotocols by which each node attempts to find its ownroute to the center. As secure data aggregation requires more computing resources and introduces additional delay overhead, existing work focuses on secure data aggregation protocols for theAMI network whose communication traffic is less timecritical[18,19]. A recent approach in[18]constructs a spanning tree rooting at the collector device to cover all of the smart meters. Aggregation is performed in a distributed manner in accordance with the aggregation tree in which

each node collects data samples from its children, aggregates them with its own data, and sends the intermediateresult to the parent node. In addition, homomorphicencryption is used to protect data privacy so that inputsand intermediate results are not revealed to smart meterson the aggregation path.

CONCLUSION

Cyber security in the Smart Grid is a new area of research that has attracted rapidly growing attention in thegovernment, industry and academia. In this paper, we presenteda comprehensive survey of security issues in the Smart Grid. We introduced the communication architecture and discussed attackand defense approaches in the Smart Grid.We also summarized the design of secure network protocolsto achieve efficient and secure information delivery in the Smart Grid. As we have reviewed, cyber security is still under developmentin the Smart Grid, especially because informationsecurity must be taken into account with electrical powersystems. Consequently,the Smart Grid requires fine-grained security solutionsdesigned specifically for distinct networkapplications, making cyber security for the Smart Grid avery fruitful and challenging research area in the future.

References

[1] J.-W. Wang and L.-L. Rong, "Cascade-Based Attack Vulnerability on the US Power Grid," Safety Science, vol. 47, no. 10, pp. 1332-1336, Dec. 2009.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," IEEE Proc., vol. 100, no. 1, pp. 210-224, Jan. 2012

[3] J. McGhee, and M. Goraj, "Smart High Voltage Substation Based on IEC 61850 Process Bus and IEEE 1588 Time Synchronization," IEEE Smart Grid Communications (SmartGridComm), pp. 489-494, Oct. 2010.

[4] G.N. Ericsson, Cyber security and power system communication –essential parts of a smart grid infrastructure, IEEE Transactions on Power Delivery 25 (2010) 1501–1507.

[5] A.R. Metke, R.L. Ekl, Security technology for smart grid networks, IEEE Transactions on Smart Grid 1 (2010) 99–107.

[6] Ricciato, F. Coluccia.A, &D'Alconzo.A ". A review of Dos attack models for 3G cellular network from a system design perspective. Computer communication 33(5),2010, 551-558.

[7] Yang.Y,McLaughlin,K. Littler, T. Sezer, S. Pranggono, B & Wang H.F , " Intrusion detection system for IEC60870-5-104 based SCADA networks. In proceedings of IEEE Power and Energy Society General Meeting?(pp.1-5).

[8] Samineni N.R., Barbhuiya, F.A Nandi,Stealth and semi-stealth MITM attacks, detection and defence in IPV4 networks.In proceedings of the 2nd IEEE international conference on Parallel Distributed and Grid Computing 2012, pp.364-367.

[9] Liu.Y, Reiter,M.K, &Ning, P, "False data injection attacks against state estimated in electric power grids. In Proceedings of 16th ACM conference on computer and communication security, 2009.

[10] IEC, Communication networks and systems in substation -- Specific communication service mapping. IEC 61850.8, 2008.

[11] PI MBUS 300 1996, Modicon Modbus Protocol Reference Guide ,http://www.eecs.umich.edu/~modbus/documents/PI_MBUS_300.pdf.

[12] Official URL for Modbus Protocols, www.modbus.org.

[13] Introduction to MODBUS , June 02, www.sena.com/support/technical_tutorial/

[14] M. Majdalawieh, F. Parisi-Presicce, D. Wijesekera, DNPSec: Distributed network protocol version 3 (DNP3) security framework, in: Advances in Computer Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, 2006, pp. 227–234.

[15] L.H. Jeffrey, H.G. James, C.P. Sandip, Cyber Security Enhancements for SCADA and DCS Systems, Technical Report TR-ISRL-07-02, University of Louisville, 2007, pp. 1–27.

[16] G. Gilchrist, Secure authentication for DNP3, in: Proc. of IEEE Power and Energy Society General Meeting (PES '08), 2008, pp. 1–3.

[17] IEC Standard, IEC 62351: Data and Communication Security.

[18] F. Li, B. Luo, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.

[19] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A.Kountouris, D. Barthel, Secure lossless aggregation for smart grid M2M networks, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.