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 are in 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, we present a review on various IDS (Intrusion Detection System) used in anomaly detection for cyber security of substations in power grid and a comprehensive survey on cyber 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 issue as millions of electronic devices are interconnected throughout critical power facilities, that relays based on the immediate impact on reliability of widespread infrastructure. Securing the advanced substation 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. Figure 1 shows the network architecture in smart grid.

Substation automation on IEC 61850 is a key element to achieve interoperability in smart grid. IEC 61850 models provide 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. 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.

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. 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. MITM attack which acts as a trusted node and communicates between the two nodes, it drops the packets. Reply attack, session hijacking, Injection 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, which provides client/server communication between devices connected on different types of buses or networks. The industry’s serial de facto standard since 1979, truly open and the most widely...
used network protocol in the industrial manufacturing environment. The Modbus protocol provides an industry standard method that Modbus devices use for parsing messages. The Internet community can access Modbus at a reserved system port 502 on the TCP/IP stack. Modbus is used to monitor and program devices; to communicate intelligent devices with sensors and instruments; to monitor field devices using PCs and HMIs [13].

B. DNP3

DNP3 is extensively used for both intra and inter substation communications in US power systems[13]. It was designed to transfer message without any security mechanism. Since it is not very practical to upgrade all legacy DNP3-based power systems into new ones in 1 day, it is essential to modify or even overhaul DNP3 to adopt more security functionalities to make a large number of legacy power devices keep pace with security requirements in the Smart Grid. Researchers [14, 15, and 16] have already started to design security functionalities for DNP3 based on two main solutions: (1) modify the original protocol to introduce security mechanisms to the DNP3 stack and (2) insert a security layer between the TCP/IP layer and the DNP3 protocol stack. The former will provide the security suits only for DNP3 regardless of the lower layer configuration; however, it needs tedious modification of the protocol stack and requires the upgrade of communication systems in power devices. The latter does not need to change 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 a security layer between DNP3 and TCP/IP is more desirable to make legacy devices compatible with smart grid devices. Specifically, the objective of this security layer is to help the DNP3 protocol achieve basic security requirements for integrity and confidentiality. At the transmitter, the security layer intercepts DNP3 packets distributed to the TCP/IP layer, encrypts the data, then sends encrypted packets into the TCP/IP layer. At the receiver, the security layer decrypts data packets from the TCP/IP layer, and passes them to the application layer (DNP3 layers). Either symmetric or asymmetric algorithms can be used to provide protection of integrity and confidentiality for DNP3 packets. For example, MAC-based authentication is designed and implemented in [16] as a security extension to DNP3-based communication for distribution automation systems.

C. IEC 61850 and IEC 62351

IEC 61850 and IEC 62351, a recent standard for substation communication, comes without its own security mechanisms. The security of IEC 61850 relies on IEC 62351 [17], which is a standard proposed to handle the security for a series of protocols including IEC 61850. In the following, we briefly discuss how IEC 62351 enforces security for IEC 61850. IEC 62351 defines both authentication and encryption mechanisms for IEC 61850 communication.

1. An authentication and encryption layer above the TCP/IP layer. This layer enforces TLS to use symmetric cryptography and MACs for message confidentiality and authenticity. This layer is intentionally used for least time-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 time-critical messages in IEC 61850 that do not pass through the TCP/IP layer, i.e., GOOSE and SMV. To ensure that such messages can be delivered in a timely manner, IEC 62351 defines no data encryption mechanism for this layer, thus time-critical messages in IEC 61850 are only protected for authenticity.

![Figure 2: IEC 1850 with IEC 62351](image)

Compared with secure DNP3, Modbus, IEC 61850 with IEC 62351 is a modern power communication protocol that balances the tradeoff between security and time-criticality by using two distinct security layers for different message types in power systems. It can be expected that more comprehensive security layering mechanisms will be proposed to achieve 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 routing protocols by which each node attempts to find its own route 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 the AMI network whose communication traffic is less time-critical [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 intermediate result to the parent node. In addition, homomorphic encryption is used to protect data privacy so that inputs and intermediate results are not revealed to smart meters on the aggregation path.

CONCLUSION

Cyber security in the Smart Grid is a new area of research that has attracted rapidly growing attention in the government, industry, and academia. In this paper, we presented a comprehensive survey of security issues in the Smart Grid. We introduced the communication architecture and discussed attack and defense approaches in the Smart Grid. We also summarized the design of secure network protocols to achieve efficient and secure information delivery in the Smart Grid. As we have reviewed, cyber security is still under development in the Smart Grid, especially because information security must be taken into account with electrical power systems. Consequently, the Smart Grid requires fine-grained security solutions designed specifically for distinct network applications, making cyber security for the Smart Grid a very fruitful and challenging research area in the future.

References