SECURITY ASPECTS ON PMU DATA COMMUNICATION BASED ON IP NETWORKS IN SMART GRIDS

Tiago Antônio RIZZETTI
UFSM – BRAZIL
rizzetti@redes.ufsm.br

Luciane Neves CANHA
UFSM – BRAZIL
luciane.canha@ufsm.br

Rafael MILBRADT
UFSM - BRAZIL
rmilbradt@gmail.com

Jeann Carlo RAGUZZONI
UFSM – BRAZIL
moothz@ufsm.br

ABSTRACT

This paper aims to conduct a discussion on the main physical media used in communications networks in Smart Grids considering PMU applications. To achieve it, a comparison of the security implications of the major physical means and technologies used in communication networks based on IP is performed. To perform this comparison, is first conducted a study of the existing vulnerabilities in a network data communication. From this, an assessment of physical media, protocols and routing technologies used under the security context of communication will be held.

INTRODUCTION

There is a great diversity of applications present in a Smart Grid, each with its own specific characteristics for requirements to data communication network. An example of these applications is the phasor measurement devices (PMU).

The PMU are becoming increasingly widespread instruments in monitoring of power systems. Primarily used in control of transmission systems to monitoring and protection through accurate measurements of voltage phasor that these devices allow. Now they are also being applied in smart distribution networks given the increase in interest from the phase angle measurements. This is due the most dynamic loads and the higher penetration of distributed energy resources (DER), which make these phase angle values, previously overlooked, important for real-time control. Beyond of these goals there are other applications relating to protection as the detection and location of faults, which can be much more precise with the use of phasor measurement capabilities.

The PMUs, in turn, have a measurement capability of dozens of samples per second, as established in the standard C37.118 [2]. To be able to exploit the full potential of the equipment there is a need to have this information available in real time. Some issues need to be considered to communication in particular the security of communication. A trend concerning in the communication networks is the use of open and consolidated standards predominantly IP networks.

The security in a smart grid has a critical importance even higher than in the current Internet. So, to deploy techniques already applied in the area of Information Technology (IT) and telecommunications (TELECOM) must be analyzed the security risks that they can bring to the system [15]. The security has several aspects to be considered and that can basically be classified into three major groups: a) privacy or confidentiality, b) data integrity and c) availability.

This work performs a discussion about communication networks used in Smart Grid focusing on applications of PMU and physical media used. For this purpose, promotes a discussion of these vulnerabilities and some techniques that can be employed to minimize security risks.

COMMUNICATION REQUIREMENTS FOR PMU IN SMART GRIDS

The PMUs are very important for fault detection in power distribution system. Through early detection of possible problems the system can perform self-healing to minimize or even avoid these problems. However, to make this possible an extensive sampling of PMUs data distributed throughout the power grid is needed. The standard IEEE C37.118 [2] addresses the issue of operation, frequency of sampling and other issues about PMU operation. The standard IEC / TR 61850-90-5 [4] deals with the use and transmission of PMU messages, meeting the requirements of the standard C37.118.2 [3] encompassing issues about communication networks in accordance with the parameters of IEC 61850.

The format of PMU message's are defined within standard C37.118.2 [3], and have different sizes depending on the message type. The message class is basically one of the following: data, configuration or command. The most common messages are data messages, which contains the readings performed by the PMU. The message's size is variable, containing around 50 bytes of payload. Its sampling rate is variable, but the standards provide that these amounts can reach 180 frames / sec [4]. Other message types, like configuration messages with hundred bytes, are infrequent messages. The command messages usually have a low frequency and small size too[3].

All PMU messages have the need for strict requirements of latency and packet loss. All communication of a PMU is considered as an real-time communication, and as such, should prioritize primary traffic, avoiding packet retransmission. The protocols used to data transport can be both UDP and TCP, but as in any real-time application,

it is preferable to use the UDP protocol. Since it causes lower overhead. The messages sent by PMU devices can be addressed either to specific recipients, using unicast, how to groups of recipients by using an protocol to control multicast group [3] [4].
About latency times, as is described in IEC / TR 61850-90-5 [4] there are different latency times used by different PMU functions. The most restrictive application, must have less than 20 ms latency. For other applications there is the possibility of higher latencies. For instance, to state estimation is allowed latencies of up to 5s. The permissible delay to messages of Sync-Check type, goes from 50 to 100 ms. These are the most common messages from PMUs.
Because of these requirements, it's possible to calculate the throughput required for each PMU device, mainly in its most frequent application (sync-check). For a payload of 50 bytes [3] in the PMU application, using an IP network at least 52 additional bytes are required for the data link layer, network and transport headers. Considering a maximum sampling rate of 180 samples/s where each message has 102 bytes, already included the overhead caused by the protocols stack, the transfer rate required is around of 18Kb/s for each PMU device. There are even other message types: configuration and command. These kind of messages presents low frequency, but anyway should be reserved enough bandwidth to all PMU messages including syn-check, command and configuration messages. Depending on the distance and quality of communication lines used by the path traversed by the messages, is possible group these messages. Considering sampling rates in the order of 180 samples per second, each sample has a 5 ms of interval each other. By the tolerance of delay for delivery of the message be up to 50 ms, one could group a set of messages and still be able to meet this requirement. If the average latency is, for instance, 10 ms, its possible group them into packets with at least 6 messages. This way, it will be transmitted together, keeps further latency lower than 50 ms and, due to the grouping, decreases the overhead caused by stack of TCP / IP protocols.

PHYSICAL MEDIA

In the context of Smart Grids, there are many different scenarios where the communication devices should be present. The number of devices present and the amount of information they transmit depend on the type of application. The PMUs, as discussed in the previous section, exhibit considerable frequency of measurement, but its concentration usually occurs in substations. By another side, devices such as smart meters, are deployed in large numbers, but the data sampling frequency is low. The area where the devices should be deployed, the criticality of the data submitted by it and its number are issues directly related to the type of physical medium used and the security to be provided.
Communications through wired means represent the most reliable currently available. The optical fiber usually used has an error rate of around 1 bit for each 10^{11} bit transmitted [7]. Moreover, it is not affected by electromagnetic interference, nor by power lines or any type of electromagnetic waves. For access to this physical medium is required peer to peer connection. Which means offering enhanced security, since an attacker cannot intercept data or interfere without a physical connection.
Further, the wired communications can consider the Power Line Communication (PLC). However, for being used is necessary to make changes in the power grid [12], and in the case of power supply interruption for any reason, the communication network also stops. This is a problem in a system which has high availability requirement.
The wireless communications, moreover, possess a number of characteristics which require more care to security [7]. Due to use a shared physical medium, there is no way to restrict access to it. Thus, even non-participating elements of communication can interact with the communication channel used. This brings a number of complications, the first one is related to data privacy. Any element that is within range of the transmitted signal can intercept that signal. If the data is not encrypted any attacker can access them [7] [12].
Another critical issue on wireless communications is the availability of the physical layer for communication. To affect the availability of a communication service is sufficient that an attacker could send invalid transmissions, on the same communication channels.
There are a wide range of technologies and coverage areas for wireless communication. From computer networks using the IEEE 802.11 a/b/g/n to the wireless sensor networks (WSN) with technologies based on the 802.15.4 standard, such as 6LoWPAN and ZigBee [12]. In addition to differences in the communication range radius there are also issues concerning the communication speed and power used to make these transmissions [17]. This is a common concern in WSN, which is certainly present in Smart Grids.

VULNERABILITIES ON SMART GRIDS

Currently, the communication devices used in power systems are converging to use IP-based communication networks [15]. These networks are widely known and there are numerous solutions for their use. However, in the Smart Grids environment there are peculiarities related to security beyond those, which are present in the public Internet.
Security issues, although important in many communication networks, acquires a sphere of critical importance in Smart Grids. It ranges from issues of privacy and data integrity to quality and availability of applications and the communication network. The following are some of the main vulnerabilities that could be exploited by attackers [17].

Privacy

Due to the two-way flow of data from smart meters, information on consumption patterns, types of equipment used, among others can be informed to utility. Because of the heterogeneity of these communications in a Smart Grid, and the different administrative domains of the networks, the possibility of interception of this information is a threat to consumer's privacy.

On PMU messages, the main concerns are about authentication on the device. Through it's allowed make changes to your configuration or obtain non-public information. To the measurement data of PMU, privacy is not a big problem because there is no information about specific clients who are to be protected. However, ensuring their integrity is essential and a potential severe problem.

Integrity

The system state is basically defined according to the measurements made by the various measuring devices distributed on the power grid, including PMUs. Based on the information obtained, the system state can be modified to work around problems presented. However, if the reported data are incorrect the system could be in an inconsistent state, causing damage to the power system or even causing customer outages.

The communication protocols used by different applications of Smart Grid must follow patterns, which are usually public. The pattern associated with the PMU messages, as described in section 2, is based on standard C37.118.2 [3]. These standards are recognized by packet analysis tools such as WireShark. An attacker could intercept messages sent by PMU devices and adulterate them by modifying the readings found. Based on this information the SCADA system could trigger events that would lead the system to an unstable state. Note that the fact that the attacker simply read the messages there is no risk. But the ability to adulterate them or generate false messages and insert them on the network through an package builder, like PackEth, for example, poses a serious threat.

Availability

A communication network for Smart Grid has intrinsic needs for high availability. Real time applications, such as the PMUs, require low latency and high availability of communications. To affect the availability, is not even necessary for an attacker to invade the network. He can just overload the access medium to the communication network, causing communication failures [12].

The availability of the communication services can be affected at various levels, from the physical layer until the application layer of the OSI model. In the physical layer the interfering signals are the problem, which hinder or prevent the communication. One example is the jamming [12] on a wireless network. In this case there is no prejudice the privacy or integrity of the data, but basically in denial of the communication service. At the application layer there are several well-known vulnerabilities in IP networks. Basically the techniques are concentrated in launching large number of requests to legitimate services to overloading them, failing to meet the legitimate requests. The Denial of Service (DoS) and Distributed Denial of Service (DDoS) [17][15] are attacks toward that end. The first one is basically obtained from a single source which makes several requests until the service is down. It is usually easier to detect and control through the filter software. But the DDoS, due to the large number of customers making requests, is more difficult to detect and control due to the similarity with legitimate customers. Usually a DDoS attack is launched by a Botnet.

Another potential vulnerability is in the network layer of the OSI model, specifically in relation to routing infrastructure [17]. To make possible communication between different networks it is necessary that the routing tables are being set up correctly. These tables are built by control algorithms and exchange of routing information, responding quickly and automatically to changes in the network topology. For this to be achieved, the different routers must communicate to each other using a common use routing protocol such as RIP, OSPF, BGP, etc [7]. If control messages of the routing tables are interrupted, or even tampered, the system will present routing problems and could making it unavailable.

There are still latency issues that directly affects the availability of a network [1]. Applications with severe restrictions latency, as PMU metering are especially critical. Even in networks that are not under attack, there could be latency issues. If the communication link is overloaded, there will be the formation of queues in network switches. Thus the data will delay. In addition, the physical layer used for transmission in many segments are shared. Different data streams compete for the use of the physical media and may exceed its capacity. Flows of high importance as the PMU data could be affected by less critical data flows, as Advanced metering infrastructure (AMI) data. These delays can be large enough to make communication ineffective. In IP-based networks this is a well-known problem in critical applications [1] [7].

SECURITY COMMUNICATION

Communication networks necessary to Smart Grid are usually composed of several networks under different administrative domains and different security policies [15]. Figure 1 shows a typical scenario of connection between the different devices. Elements of great importance and present in smaller quantities, such as substations, are typically interconnected through trusted connections. These are obtained from ISPs (Internet Service Providers), that connect them, usually through optical fiber, to the Internet infrastructure. Other IEDs

present in the distribution network shows lower concentration, greater quantity and geographical dispersion. For these devices the use of mesh networks [15] [17] can be an alternative. Each element can communicate with its neighbors, this way creating communication paths between these devices. The mesh network could use gateway in some points to connect it to the Internet.

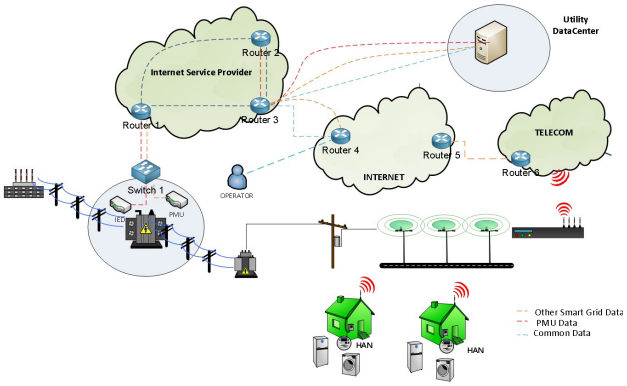

Figure 1: Smart Grid Scenario

The PMU devices, because are present on substations, has a higher availability in relation to the physical layer. However, on the ISP its flows will dispute with the data from other sources, such as system operators, measurement data, among others. There are a set of techniques called QoS (Quality of Service) which allows improvement in the reliability of communication when there is shared networks [1] [7].

To provide secure communication, elements that are used on the Internet can be used in Smart Grids [15]. Aspects of privacy and data integrity could be obtained through the use of encryption in messages [7] [15]. Concerning to the availability is needed to treat it from the physical layer of the OSI model to the application layer. At the physical layer, in a shared media, like that used in wireless communications, many techniques can be used to ensure security to the physical media, as described in [13] [14]. Already the level of service availability, the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are the most suitable [9]. Through access to network profiles a system can be choose to block messages that come through that network. In the work presented in [4], the author proposes the creation of a distributed firewall to be deployed in all IEDs in the network, forming a secure means for blocking unauthorized equipment.

The use of IP-based networks, allow the use of security technique called IPSec [7] [9]. It can be used in two ways: a) directly on IEDs;. b) directly in the routers used by them [15]. IPSec uses asymmetric key encryption. It means security, but demands processing power on the device where it is present. Often IEDs are devices that have limited processing power or must have low power consumption. Thus, implement IPSec directly in IEDs cannot be a suitable choice in most situations. By other side the implementation of IPSec at routers on which the IEDs are connected is a solution with ease of implementation, since all processing is performed by routers. These devices are dedicated to network traffic, and has better processing capabilities.

The use of Virtual Private Networking (VPN) techniques [7] [9] are also alternatives that can address the privacy and integrity of the Smart Grid data. Especially in the case of data being transported by the public networks. Moreover, one can use a technique similar to circuit switching supported by IP-based network, the Multiprotocol Label Switching (MPLS) [10]. This type of technique creates communication circuits in the data link layer (L2) of the OSI model. Once the circuit is established, it works like a tunnel, always following the same path. Its data can only be accessed on tunnel's end, what contributes to the confidentiality and integrity of transmitted data. The MPLS technique associated with resource reservation through the RSVP protocol (Resource Reservation Protocol) in their versions Traffic Engineering (TE) may also contribute to the increased availability [1]. It ensures the necessary resources in each node for data messages critical, such as the measurement information by PMUs.

The access to IEDs must be performed by authorized personnel only. Therefore one must have an authentication mechanism, authorization, and accounting (AAA) [7] [15]. The access to the devices must be through individual access credentials and can use mechanisms of access profiles and permissions. A centralized database can be used as a Remote Authentication Dial In User Service (RADIUS). However there must be the possibility of access to devices via the local network [15]. That is, even in a failure situation in the communication network, from the local network the operator should be able to access the device allowing control, configuration and data collection.

To validate security solutions used its performance must be verified. To achieve this should be used softwares for security analysis. Robustness testing of protocols and softwares used are extremely important to ensure that none link of security chain be weak. Thus, security is guaranteed, especially with regard to system availability.

CONCLUSION

Given the trend of using IP networks, the issue of providing a communication with high security and availability for the applications is critical to the success of its use. To improve the quality of energy and services provided by utilities is essential monitor the system in real time through the PMUs and other applications to know their precise status. Given this information, operators or supervisory systems can make decisions while maintaining the integrity of the power system. For

this to be possible, two-way communication networks with high security and high availability are essential. The use of techniques already used in the Internet network can be used, but must be assess the risks that these offer this type of environment.

ACNOWLEDGEMENT: The authors would like to thank FAPERGS for financial support to this research.

REFERENCES

[1] Salsano, Stefano; Botta, Alessio, Iovanna, Paola, Intermite, Marco; Intermite, Andrea. *Traffic Engineering with OSPF-TE and RSVP-TE: flooding reduction techniques and evaluation of processing cost.*

[2] IEEE Standard C37.118-2005 (Revision of IEEE Std 1344-1995) "IEEE Standard for Synchrophasors for Power Systems". *IEEE Standard for Synchrophasor Data Transfer for Power Systems.*

[3] *IEEE Standard for Synchrophasor Data Transfer for Power Systems, IEEE Std C37.118.2TM-2011.*

[4] *IEC 61850 Standart. Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118.*

[5] Juho Markkula, Jussi Haapola. Impact of Smart Grid Traffic Peak Loads on Shared LTE Network Performance. *IEEE ICC 2013 - Selected Areas in Communications Symposium.*

[6] Elias Bou-Harb, Claude Fachkha. Communication Security for Smart Grid Distribution Networks. *IEEE Communications Magazine , January 2013.*

[7] ROSS, K.; KUROSE, J. *Computer Networking: A Top Down Approach.* Pearson, 2010.

[8] Zhuo Lu Xiang Lu Wenye Wang. Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid. *The 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management*

[9] Oppenheimer, Priscilla. *Top-Down Network Design. 3th Edition: A system analysis approach network design.* Cisco Press. 2010.

[10] Internet Engineering Task Force. *RFC 2702. Requirements for Traffic Engineering Over MPLS.*

[11] The Internet Society. *An Architecture for Differentiated Services. RFC 2475.*

[12] Xudong Wang; Ping Yi. Security Framework for Wireless Communications in Smart Distribution Grid. *IEEE Transactions on Smart Grid, VOL. 2, No. 4, December 2011.*

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans Wirel. Commun., vol. 7, no. 6, pp. 2180–2189, 2009.*

[14] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans Inf. Theory, vol. 54, no. 6, pp. 2735–2751, June 2006.*

[15] NIST Smart Grid Cyber Security Working Group, "*Guidelines for smart grid cyber security: Vol. 3, Supportive analyses and references*," NISTIR 7628, Aug. 2010.

[16] M. S. Esfahani. *Security Analysis of Phasor Measurement Units in Smart Grid Communication Infrastructures.* Dissertation In Partial Fulfilment of Requirements for the Degree of Master of Science, University of Nebraska – Lincoln. May 2014.

[17] W. Wang; Z. Lu. Cyber security in the Smart Grid: Survey and challenges. *ELSEVIER - Computer Networks 57 (2013) 1344–1371.*