PMU AVAILABILITY AND SECURITY IN SMART GRIDS BASED ON IP PROTOCOL

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

Pedro Bastos ZORRILLA
UFSM – BRAZIL
pbzorila@inf.ufsm.br

Alzenira da Rosa ABAIDE
UFSM – BRAZIL
alzenira@ufsm.br

Cesar AREND
UFSM – BRAZIL
cfarend@inf.ufsm.br

ABSTRACT

Communication networks consists of a crucial tool for the implementation of Smart Grids. The different kinds of data flowing in a Smart Grid have different latency and reliability requirements. Phasor Measurement Units (PMU) are becoming increasingly widespread like instruments to monitoring of electrical distribution systems. The use of this equipment has severe restrictions on bandwidth, latency and packet loss. The trend for the use of IP networks makes imperative the use of mechanisms to ensure treatment to these requirements within implementations of Smart Grids. This paper realizes an approach of QoS mechanisms available to increase the availability, reliability and security in the context of PMU applications within Smart Grids.

INTRODUCTION

Phasor Measurement Units (PMU) were initially applied in transmission system to provide control, monitoring and protection through accurate measurements of phasor voltage on these devices. In nowadays these equipments are also being applied in smart grids due to the increased interest in measures of phase angle. This increase in interest in phasor measurements is related to the great dynamism of loads and high penetration of distributed energy resources (DER), which make these values of phase angle, previously neglected in distribution systems, important for real time control. Despite this application be related to state estimation there are other applications related to security such as detection and faults location, which can be much more accurate with the use of phasor measurement capabilities.

The PMUs, in turn, have a capacity of measuring tens of samples per second, as stipulated in the standard C37.118 [2]. To be able to exploit the full potential from this technology is important to have this information available in real time (RT). So, some communication issues such as bandwidth, latency and reliability provided by the protocols should be considered. The actual trend concerning the communication networks is the use of open standards predominantly based on IP networks.

Wherefore PMU messages can be efficiently used to provide protection to the electrical system, the latency required to this application is about a few milliseconds. This way requiring adequate mechanisms to maintain this latency level. The communication networks based on IP protocol, are inherently designed to work performing best effort to deliver packets, but without any guarantee. To avoid this problem QoS (Quality of Service) [9] [7] mechanisms should be employed to prioritize traffic within this network, reducing and keeping under control the communication latencies. This feature is especially needed when using networks where there is other traffic data, such as convergence to the same communication network of other systems of monitoring and control presents in the electric power system.

The purpose of this study is to discuss QoS techniques available in IP networks such as the use of MPLS (Multiprotocol Label Switching), RSVP (ReSource ReserVation Protocol), 802.1p and DSCP (*Differentiated services code point)* protocols from the perspective of intelligent networks focusing on the use of PMU data communication and associated issues with it. Criteria such as real-time traffic and the size of the packets should be considered and through simulation of the system with the application of restrictions as sampling frequency, could define the most appropriate techniques for these environments.

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 are needed a extensive sampling and

data collection of PMUs distributed throughout the power grid. The standard IEEE C37.118 [2] address 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 messages are defined within standard C37.118.2 [3], and have different sizes depending of message type. The message class is basically one of the following: data, configuration or command. The most common messages are the data, which contains the readings performed by the PMU. The size of this kind of message is variable, containing around 50 bytes of payload. Its sampling rate is variable, but the standards provide that these amounts can reach the house of 180 frames / sec [4]. Other message types, like configuration messages, has hundred bytes, but are infrequent messages. The command messages usually have a low frequency and small size [3].

All PMU messages have the need for strict requirements on 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 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. The protocol stack used can be viewed in Figure 1. Considering a maximum sampling rate of 180 samples / s where each message has 102 bytes, already included the overhead caused by the protocol stack, the transfer rate required it's around 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, its possible even group them. 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 grouped. This way, it will be transmitted together, further keeps latency lower than 50 ms and, due to the grouping, decreases the overhead caused by stack of TCP / IP protocols.

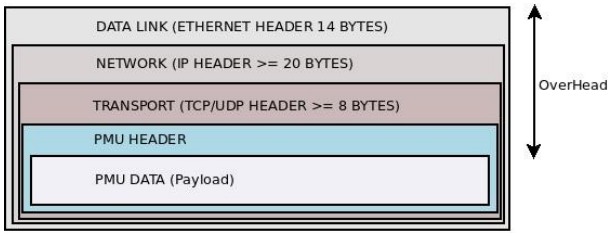

Figure 1: Packet Structure and Overhead.

OVERVIEW OF QUALITY OF SERVICE (QOS) ON IP BASED NETWORKS

The packet switching, used in IP networks, is based on the premise that each packet on a communication flow may follow a different path to get your destination. This feature is quite interesting when analyzing the aspect of fault tolerance of the communication network. Even if some element on the path used by a data flow has problems, each packet is routed individually. So if the network it's able to detect another possible path, it will be used keeping the transmission. This characteristic of functioning despite providing considerable resilience, entails some problems, including [7]: a) possibility of delivering packets out of order b) There is no guarantee of packet delivery c) No guarantee of latencies and jitter about this communication.

In an ideal situation, where the communication network isn't overloaded, all packets are transmitted without queuing and therefore without delays beyond those necessary by the data transmission on the physical layer. However, it is a common situation a communication network show a resource competition, especially in situations with an very high utilization rate, beyond

your capabilities. So in this case packets are usually enqueued. This adds an extra delay on communication. In some situations this is very critical issue. Worth remembering that the closer to 100% is utilization of the network, the larger is the queuing. In fact, the queue grows exponentially [9] with network loads. Therefore, it is necessary to use techniques that limit their size, preventing an uncontrolled growth of these queues.

Due to the difficulties imposed to increase the physical layer capacity in all overload situation, it's necessary to prioritize some types of data more important than others [7] [9]. Figure 1 shows the described situation, since any communication between group A and B must pass through the link which have only 1 Mbps. This rate is lower than the other communication links at this scenario.

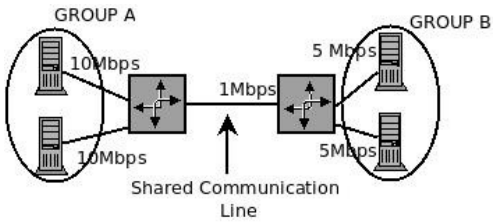

Figure 1: Shared Communication Lines

There are ways to address these problems in IP based networks, through the use of a set of technologies and protocols called QoS (Quality-of-Service). There are basically two classes of QoS in IP networks: the Integrated Service (IntServ) and Differentiated Service (DiffServ). The first makes use of a resource reservation on the path to be traversed by the data stream. So, ensuring that there are sufficient resources for a successful communication. The diffserv techniques acts on a different way. It offers no guarantee of transmission, however provides a priorization of data traffic from important applications.

QOS TECHNIQUES APPLIED TO PMU APPLICATION

There is a trend in the convergence of communications networks to IP based networks, since this networks has a widespread use. In the context of smart grids, communication networks used by the PMUs may be shared with other applications used in the Smart Grid or even with others kind of data [5]. The QoS technologies should been applied for ensuring that priority data, such as messages from the PMU, are prioritized to ensure the integrity of the power system.

There are several possible scenarios to the use of IP networks on Smart Grid communications. Being the most realistic scenarios those one that use shared networks. This sharing can be accomplished in two ways: a) in the context of a exclusive network for all applications which belongs to the smart grid, b) applications beyond all the applications that make up the Smart Grid, adding further data streams, not related to Smart Grid, from common users. In the case of a shared network for Smart Grid applications and common users, there is still two options: the first uses the network telecommunication infrastructure of a telecom operator. In the second form, a network is built for the Smart Grid, and she is harnessed for use by customers of the utility in regions where there are difficulties for operating telecom services, such as in rural areas. Figure 2 shows a scenario designed to simulate different kinds of data possible on the communication network.

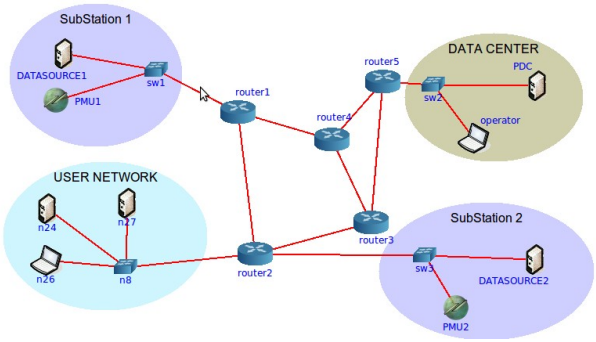

Figure 2: An example of Smart Grid with Shared Communication Network

For each substation there a PMU and another automation network data related to the power distribution system. For instance, these automation network data could belong to: smart meters, remote controlled switches, etc. These data are transported to the data center of the utility. There their software can receive the data and make the necessary processing. It is noteworthy that the data center may be geographically remote from the substations. To transport these data, could be used an IP-based network, through routers that interconnect several networks. These elements can manage of different data flows from several substations, besides flows from ordinary users, in the context of a shared communication network.

To provide the required network throughput for specific applications isn't enough just increase the total network throughput. One should ensure that the correct applications make use of this throughput. The QoS techniques can be applied to ensure this, on different levels in the stack of TCP/IP protocols. It's even possible combine techniques and apply them in different

levels. Thus, promoting a better and broader priorization, covering from internal network segments to the internet connection. The following it's described some of the techniques mostly used in IP networks.

Use of VLANs

VLAN Techniques defined in the IEEE 802.1Q standard, are used for various purposes in the context of communication networks. It's used since to improve security until to improve network performance. This technique is used to create virtual networks independent of the geographical location where the communication devices are. Each network frame has 2 bytes added to it, the information added consist on a VLAN identifier and the frame priority, as standardized by the IEEE 802.1p. Thus, the use of VLANs, allows specify the priority that should be given to the data frame, depending on the nature of the application that it carry. In addition, the priorization made in the data link layer, using the IEEE 802.1p standard, can be used to generate marking of priorities at the network layer (L3).

Using the IP header ToS field

At the network layer, L3, of the OSI model, priorization can be performed using the ToS field (Type Of Service), the information available in this field is the DSCP [11], which specifies the priority of the packet. The edge routers, shown in Figure 2 as router1, Router2, Router3 and router5 must be configured to sort the package and mark it. In the case of PMU data flows, just mark data packets from TCP e UDP ports 4712 and 4713, respectively, marking them with real-time priority [3]. After the package marking this information may be used in other switching elements of the network.

The priorization of traffic is a practical approach to improve the performance of some applications, but not always sufficient. For a more reliable approach can be used not only techniques that prioritize data flows, but acting on the reservation of resources for all the necessary path to communication.

Using MPLS associated with the RSVP protocol

The Multiprotocol Label Switching (MPLS) technology consists of a technology similar to VLAN techniques, on the same way performs the identification of data streams, but in this case, it's between the layers L2 and L3 of the OSI model. A natural consequence of this fact is the scope of the protocol, which also operates at the network layer, thus being used as identifier for referrals between different networks. To be used, it is necessary that the equipment infrastructure of the communication network supporting this technology. A crucial part of the process consists in the way the resource reservation is performed. There are protocols responsible for this function, the most used is the Resource Reservation Protocol (RSVP). This protocol can be seen as a signaling protocol, used to configure the path in which the data will travel on. Nowadays a variant called RSVP-TE (Traffic Engineering) is used in conjunction with routing protocols such as OSPF-TE (OpenShortest Path First - Traffic Engineering) which are responsible for selecting and allocating resources [1] [7].

SECURITY ON COMMUNICATION IN SMART GRID

There are several vulnerabilities that can compromise the communication network, and bring serious consequences to smart grid as can be seen in [6] and [8]. Critical applications, such as applications of PMU and many other applications present in a smart grid are extremely sensitive to security issue. If an attacker may gain access to the network and tampering with the transmitted data or even adds incorrect data could cause serious damage to the operation of the power system. Even attack techniques based on DoS (Denial of Service) are extremely harmful to these applications. This type of attack does not change the network data, but overloads the network elements adding useless data. In a congested network, legitimate messages may be delayed beyond that permitted or even be lost. In the case of PMUs, for example, the latency of some messages must be less than 50 ms, this value can be easily extrapolated if there isn't some way to protect and prioritize these data. As a result, protection mechanisms and resilience will stop acting, compromising the integrity of the power system. Thus, traffic priorization and implementation of mechanisms to target it's essential to correct functioning of the communication network used by the applications in this environment.

The use of some of the main techniques used for QoS has the side effect of increasing the security of the system. Using VLANs, for example, by segmenting the network, in practice substantially reduces the ability of attack on a shared network. It avoids breaches of confidentiality, data integrity and availability of the network. The only way an attacker can compromise the network, would be getting access to the equipment itself where this segmentation occurs.

Another practical example is the use of MPLS-TE technology associated with RSVP-TE technology. Initially used to increase network availability and provide quality assurance in communication, it also provides higher security. The MPLS is implemented in the form of tunnels. Each tunnel, in a communication link has two well-defined edges. The tunnel data just can be accessed by one of its ends. Thus, attackers do not can access network data, unless they could get access to their ends, using the communication equipment plugged into them. On the same way, they can't insert tampered data on this. Thus, it creates a kind

of secure communication channel. The configuration of tunnels is performed automatically by the RSVP-TE protocol, according to application needs. Certainly these special tunnels cannot be used by any applications who wants to, but just by applications of critical importance, previously defined. The PMU applications are an example of special treatment that could be provided by the MPLS tunnels. Due to its operation, this technique, similar to VLAN, if well used, can help reduce security risks. Thus, reducing the possibility of data tampering, counterfeiting, and especially increasing the availability of the network, dramatically reducing the effect of DoS attacks [6] [8], and potentials bottlenecks that may occur.

Given the information presented, the following frame summarizes some of the key technologies as relevant aspects of QoS in IP networks. Introducing technology, network layer in which it operates, capacity to ensuring network resources, the ability to support real-time traffic (RT), ability to improve security and how it's their support at most common networking devices.

QoS Type	Layer OSI	Accuracy rule	RT Support	Security features	Widely Supported
IEEE 802.1P	L2	No	Yes	Yes, segmentation of VLANs.	yes
TOS (DSCP)	L3	No	Yes	No	Yes
RSVP-TE + MPLS-TE	L2/L3	Yes	Yes	Yes, by creating MPLS tunnels	Restricted to specific models.

CONCLUSION

Given the trend of using IP networks, the issue of providing a better experience for users and applications is critical to the success of its use. This is essential in critical applications such as the case of PMUs in the context of Smart Grids. Like previously presented, it can be said that the use of technologies that implement IntServ, such as MPLS-TE + RSPV-TE tend to show better contribution to communication quality [10]. However, it is worth noting that not all network equipment must support this technology. In this case, the use of DiffServ, which is widely supported by network equipments, its a possible choice. While not offering warranty, delivers performance improvement. Depending on the context of the network can provide good results in its implementation. It is suggested as future work the implementation of PMUs simulators and plugins to network simulators to allow full simulation of these environments.

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] I*EC 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.