2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)
Virtual, October 26-28, 2020

Bandwidth and Security Requirements for Smart Grid

Kinan Ghanem
Power Networks Demonstration Centre,
University of Strathclyde, Glasgow, UK
kinan.ghanem@strath.ac.uk

Rameez Asif
Power Networks Demonstration Centre,
University of Strathclyde, Glasgow, UK
rameez.asif@strath.ac.uk

Stephen Ugwuanyi
Department of Electronic and Electrical Engineering,
University of Strathclyde, Glasgow, UK
stephen.ugwuanyi@strath.ac.uk

James Irvine
Department of Electronic and Electrical Engineering,
University of Strathclyde, Glasgow, UK
j.m.irvine@strath.ac.uk

***Abstract*— With the evolution of smart grid and applications, power distribution networks need scalable, flexible, distributed and secure end-to-end communication. This work aims to highlight the necessary bandwidth that is needed to effectively monitor and communicate with all the secondary substations of Distribution Network Operators (DNOs). In order to determine the bandwidth requirements, the current and future applications in each secondary substation should be known. Two levels of security are employed – IPsec and TLS – to give flexibility and resilience. Different test scenarios and several setups were employed on a fully secured IP based Remote Terminal Unit (RTU) through an IEC 62870-05-104 protocol, aiming to understand the bandwidth cost of different security techniques. The analysis depicts an average of 2-3 fold increase in bandwidth if both IPsec and TLS are used be to secure the connected asset.**

***Index Terms*—Smart Grid, Spectrum, Bandwidth, IP Security, Power Utility, Encryption, Networks, TLS and Distribution Network Operators.**

I. Introduction

The smart grid requires communications for data exchange between control centres and the associated devices in the field for remote management. The heterogeneous nature of the smart grid system – numerous devices from a number of different vendors of varying age over a wide area – creates several challenges for the communication network, and makes a single unified protocol impractical. Secondary substation automation, where many devices are in the hard-to-reach areas, will need a reliable communication solution to connect field assets to the control centres. Wireless technologies provide an obvious solution for such use cases, but deploying any wireless technology will require spectrum [1]. While some wireless systems, such as LoRaWAN, rely on unlicensed spectrum, depending on such spectrum for makes quality of service difficult to guarantee. While commercial cellular operators have licensed spectrum, since utility networks are critical national infrastructure, they have far more stringent requirements than most commercial wireless networks can support. This therefore suggests the use of dedicated wireless networks provided by the utility networks themselves, which will require dedicated spectrum allocations.

Any spectrum supporting utility network provision will need to take into account not just that future applications will involve greater numbers of devices and each of these devices will require more bandwidth to give increased quality of measurement, but also that the possibility of cyber-attacks that could target the power network will increase. Cybersecurity is therefore essential for any communication deployment for power utilities. This will also increase the bandwidth requirement and in turn the spectrum allocation needed.

Various wireless and wired communication technologies have been employed in power utilities [2]. Most DNOs globally rely on a combination of more than three of these communication technologies for various grid applications and connectivity. The UK national coverage maps of Mobile Network Operators (MNOs) suffer from the lack of coverage especially in the rural parts of Scotland [3]. While the data rates needed for each RTU from DNOs differs from one DNO to another, all the existing data rates are without any security plan and recovery methods in place. While a great deal of literature exists on smart grid security, the effect of adding security on the bandwidth requirements has not been investigated.

This research work aims to investigate the bandwidth requirements for the secondary substation automation taking into consideration the security overhead caused by applying different security techniques. The results from this research are part of the University of Strathclyde Power Network Demonstration Centre (PNDC). We set up a functional testbed and monitored communications between a fully secured IP RTU (the client) and a management server. Different configurations and setups were investigated to understand the effects of adding security techniques to the existing system.

This paper is divided into four sections: Section II presents the current spectrum and security challenges facing the power utilities; Section III discusses the security and bandwidth test setup procedures; Section IV analyzes the findings; and Section V conclude the paper with key points, necessary recommendations for DNOs and highlights the

This project was funded under the core research programme of the University of Strathclyde's PNDC (https://pndc.co.uk).

future work that would focus on radio technology involving other manufacturer's RTUs.

II. Communications Challenges in Power Utilities

There are several challenges facing the deployment of any communication technology in the power utility today. Some of the main challenges include the reliability, security, availability and cost effectiveness of the communication links between the control centre and secondary substation on-field devices. Wireless technologies can be deployed rapidly and may not require complicated construction and civil works, which can make it easier to be used in different smart grid applications. Currently, power utilities globally use many different communication technologies to connect in-field devices to the control centres. The selected communication technology will be chosen based on the application and the availability of the signals, coverage and strength. UHF telemetry is widely deployed by the power utilities worldwide as an option to support Supervisory Control and Data Acquisition (SCADA) communication system to control and monitor reclosers and switches. Recently, some DNOs in the UK have deployed Broadband Global Area Network (BGAN) satellite technology to remotely control and monitor their distributed assets in hard-to-reach areas [4]. Other wireless Low Power Wide Area Network (LPWLAN) technologies such as LoRaWAN, Sigfox can be used for asset monitoring and fault detection [5].

Legacy power utility communication protocols suffer from many limitations. Some are vulnerable to cyber-attacks, while others have some drawbacks preventing them from supporting massive integration with the new applications (i.e., electric vehicle charging stations, distributed storage, distributed generation and demand response related needs for end-points). Another important point is the overhead that comes from integrating these legacy power communication protocols with the IP network, which is the underlying network protocol for establishing connection between the endpoints and central control centre. The status of most wireless technology used in connecting the secondary substation suffers from limitations such as the limited and narrowband channels, lack of coverage and integration with legacy assets.

With the evolution of smart grid and growth of the end-user applications and number of endpoints, many existing wireless technologies (such as UHF telemetry) will not be able to offer the necessary capacity. Also, the NIS Directive [6] and the security requirements of other grid applications such as Low Voltages (LV) monitoring, solid-state transformer control and active network management will drive bandwidth requirements and increase the demand. This agrees with [7] that the addition of more security mechanism increases the number of data-bytes which increase the bandwidth. The question about how much bandwidth the power utilities need to cope with the current and future smart grid requirements is not easy to answer. To provide an estimate of the required bandwidth, we carried out different scenario testing at PNDC to help understand the bandwidth required for the secondary substation taking into consideration the security overhead as illustrated in the remaining part of this paper.

A. *Requirements for Secondary Substations*

Wireless technology plays an important role in the remote monitoring of smart grid assets in the hard to reach areas. Power utilities need a real-time and reliable two-way communications network that extends beyond the distribution substations all the way to the customer premises [8]. To meet these objectives, the wireless communication networks used in power utilities must have enough capacity to support the increasing data requirements of smart grid while being highly reliable and providing low latency communications. Moreover, the technology should provide high security to prevent cyber-attacks. Other requirements include supporting legacy equipment and having a high degree of power back-up to maintain the operation during any power failure, since the communications network will be required to bring the power network back online.

When deciding which communication technologies are appropriate for smart grids, the basic requirements of smart grid communication infrastructures in terms of bandwidth and latency must be met. Additionally, non-communications metrics must be considered. These include availability, accessibility, Quality of Service, maintainability, resilience and affordability.

A particular additional requirement is power backup, which is crucial for any deployed communication technology in the power utility. The Energy Networks Association (ENA) engineering recommendation G91, issue 1, 2012 specify that substation batteries should have enough capacity to meet the standing demand for 72 hours. This will guarantee that there is adequate backup power for the site to remain in operation for at least 72 hours after a power supply loss confirming that auxiliary systems and command and control structure remain unaffected after grid failure (i.e. black start procedure after a blackout) [9,10]. For secondary substation applications, at least 24 hours of backup power are needed to maintain the operation during any unexpected loss of power scenario.

B. *Available Radio Spectrum*

Spectrum allocation is key for any wireless technology. Meeting the coverage and capacity requirements are crucial to future wireless technology for the smart grid. With enough spectrum in a proper band, rural coverage and urban capacity can be satisfied, keeping in mind that the demand for spectrum will continue to grow, as power applications interconnectedness increases. In the UK, the Office of Communications (Ofcom) is developing a strategy for managing some spectrum frequency bands over the next decade. Part of the process is to understand the bandwidth requirements for smart grid applications.

DNOs require a spectrum below 2 GHz that offers better rural coverage and better signal penetration for their remote sites. However, the available bandwidth below 2 GHz is restricted to few narrow frequency bands [11]. Higher frequency bands of more than 2 GHz suffer from several challenges and drawbacks for power utility applications. While the utilities have considerable infrastructure, access to sites suitable for mounting transmission equipment is more limited. Much control equipment is underground or in basements in cities. The limited coverage and weak signal penetration of higher frequencies would make deployment costs at high frequencies uneconomic.

In the UK, there will be several bands available below 2GHz, which could be considered as a potential option for the DNOs for any future development of a private wireless technology (Private LTE) for the smart grid. The availability of the frequency bands of 87, 88 and 31 are possible option for a dedicated spectrum for the smart grid. The advantage of such bands is the fact that the transmitted signal can better penetrate through the surrounding environment and could offer a very good coverage. However, the bandwidth will be strictly limited and may not exceed 5 MHz in each band. For example, the band 410-415 & 420-425 MHz consists of 2 x 4 MHz with 10 MHz duplex spacing, which is currently fragmented across these two 5 MHz blocks [12]. The use of this spectrum in the future may be possible if Ofcom decided to release them. However, in the face of considerable demands from other sectors of the economy, any frequency allocation decisions must be based on evidence.

III. THE BANDWIDTH TESTING SETUP

In order to determine the bandwidth requirements for secondary substations, we identified the data flow between the communicating entities. This is the SCADA polling of the RTU measurements and the protocol used to link the RTU with the SCADA control centre. The bandwidth set-up and its calculations considered the use of IEC 60870-5-104 (IEC104) protocol applied to the test setup at this stage. It is assumed that future deployment of RTU connectivity will comply with the IEC 62351, which is the security standard for substation communication, including the ISO/IEC 61850, DNP3 or IEC 60870-5-104 [13].

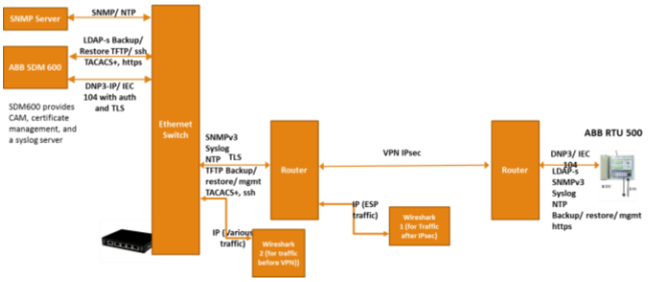

SNMP Server
SNMP/ NTP
LDAP-s Backup/ Restore TFTP/ ssh TACACS+, https
ABB SDM 600
DNP3-IP/ IEC 104 with auth and TLS
SDM600 provides CAM, certificate management, and a syslog server
Ethernet Switch
SNMPv3 Syslog NTP TLS TFTP Backup/ restore/ mgmt TACACS+, ssh
Router
VPN IPsec
Router
ABB RTU 500
DNP3/ IEC 104
LDAP-s SNMPv3 Syslog NTP Backup/ restore/ mgmt https
IP (ESP traffic)
Wireshark 1 (for Traffic after IPsec)
IP (Various traffic)
Wireshark 2 (for traffic before VPN))

Figure 1 High-level Bandwidth Requirements Testbed at PNDC

A complete setup of a fully-secured IP capability is installed at the PNDC to understand the bandwidth and security requirements (see Figure 1). The RTU is part of the ABB RTU500 series, which is IP based and designed to meet the DNO's needs in transmission and distribution automation. The RTU supports a number of different security approaches for authentication and encryption.

An example application for secondary substation automation was designed. This monitors a number of analogues and digital measurements which are transmitted from the RTU to the control centre (Slave RTU to Master RTU in this setup). It was assumed that the RTU needs to transmit 18 measurements of analogues each 10 minutes. This configuration and protocol was based on the experience of DNO members of the PNDC.

Table 1 Bandwidth Requirements Test Scenarios

	Sub Device ALL V0	Sub Device Sub A V0	Sub Device Sub B V0	Sub Device Sub C V0	Sub Device Sub D V0
IEC104 Sec	x	x			
SNTP	x		x	x	x
LDAP	x				x
HTTPS	x		x		x
Syslog	x		x		x
SNMP	x		x	x	x

Various scenarios were considered in the testing. The cyber security approaches complied with the NIS directives and IEC 62351 standards to secure the connection, increase system robustness and control user management.

Table 1 gives some of the test scenarios. Different tests were performed to check the background traffic taking into consideration activations and deactivations of the security for the IEC104. The tests were delivered over two days of different configurations for IEC104 namely: 4 analogues each 10 seconds (this test checks the connection reliability and the IPSec) and 18 analogues each 10 minutes (fully secure package for IEC 104 along with remote access and syslog with and without VPN were performed). The IEC 104 keep alive each 30 seconds is used in this test.

The VPN aspect of the testing was setup by Cisco modules via an IP tunnel between two routers to represent the connection through a wide area network (WAN). Another level of security came from activating different security approaches from the ABB RTU, namely, TLS V1.2 (i.e. LDAP, HTPPS) and syslog. The test ran over 48 hours and the data were captured via Wireshark before and after entering the VPN tunnel. The analysis of the data is described in the next Section IV.

A. Cyber Security Considerations

The bandwidth calculations considered the overhead of security requirements applicable to power utilities. Based on NIS directive [6] and compliance with the IEC 62351 standard, a connection via DNP3 and IEC 60870-05-104 should be secured. In this project, two levels of security were applied to the connection and the transmitted data. The first level is device to device between RTU and the control unit, and the second level of security is from the IPSec through a VPN between the routers.

Several security techniques/protocols can be used by power utilities for authentication, management, encryption and certificate updates. For example, the Internet Protocol Security (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications. This protocol is considered in the bandwidth calculations as a level of security when using a WAN. Moreover, TLS, Hypertext Transfer Protocol Secure (HTTPS), File Transfer Secure Protocol (FTSP) and Simple Network Management Protocol (SNMP) can also be applied to secure the connection through the smart grid. The above security protocols were applied based on the application, as some applications may not require all the above listed protocols.

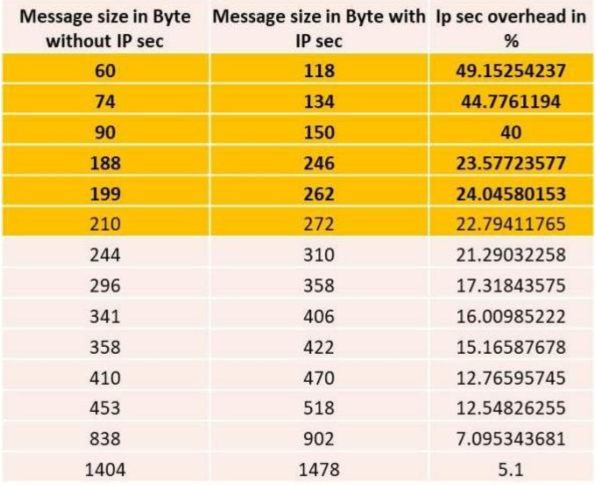
IV. Bandwidth Analysis

This section highlights the findings of the testing scenario aimed at providing answers on the IPSec security overhead over secondary substation RTU and the percentage of the TLS overhead needed to enable secured functionality of the secondary substation RTU via a reliable communication link. From the analysis of the captured data through Wireshark, the observations were enlisted and concluded.

A. *IP Security:*

The IPSec wraps each packet in a new frame securely. The new payload is encapsulated by the IPsec headers and then all packets inside the IP tunnel will appear in ESP format. The captured data shows that the exchanged messages (between the Master and the Slave RTU) have different message size, which varies between 60 bytes to 1404 bytes before entering the VPN tunnel. The captured data after entering the VPN tunnel appear in the ESP format with a message size of 118 to 1478 bytes as shown in Table 2.

Table 2 Messages Size before and after entering the VPN and IPsec overhead



Message size in Byte without IP sec	Message size in Byte with IP sec	Ip sec overhead in %
60	118	49.15254237
74	134	44.7761194
90	150	40
188	246	23.57723577
199	262	24.04580153
210	272	22.79411765
244	310	21.29032258
296	358	17.31843575
341	406	16.00985222
358	422	15.16587678
410	470	12.76595745
453	518	12.54826255
838	902	7.095343681
1404	1478	5.1

The analysis of all scenarios shows that small message size is observed more frequently than the big message size (e.g. greater than 200 bytes) for all the scenarios and testing run at PNDC. Table 2 shows the overhead caused by the IPsec for different message size.

Table 3 Estimated Bandwidth Based Protocols

Protocols	Bandwidth (%)
SNMP + NTP + ICMP	07 – 11
IEC 104 ASDU and IEC 104 (keep-alive) each 15 sec	15 – 19
TCP	13 – 17
TLS V1.2 (remote access, HTTP over TLS, background security traffic and full security from ABB)	29 – 39
IPSec (VPN tunnel)	12 - 38

The main finding from such comparison (for different scenarios and setups) is that the IPsec for small size packets (i.e. TCP, IEC 104 keep-alive, handshake protocol and 104 APCI packets) will add more than 25% overhead to the packet size, as most of the captured data are less than 200 Bytes. When activating TLS for remote access and role-based access control authentication (i.e., https and LDAP), the packet size of TLS v1.2 becomes larger than the captured data before activating TLS for remote access. As a result, the IPsec overhead will not exceed 15% (for TLS captured packets with more than 360 bytes). The packet size determines the percentage of the IPsec overhead. Configuration and application affect the packet size which in turn also affects the IPsec overhead.

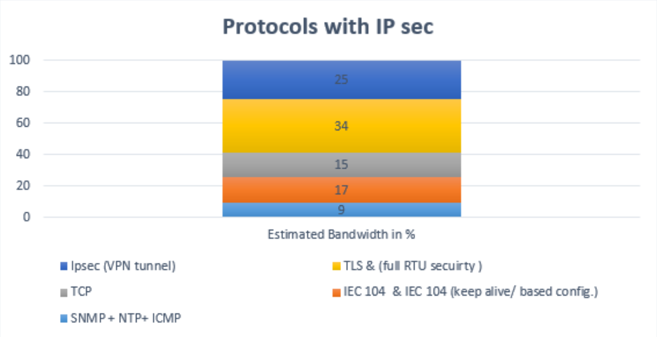


Figure 2. Average Bandwidth per Protocol

Another observation from the analysis over different scenarios and setups shows that the overhead attributed to IPsec will vary based on the message size. Smaller message sizes will result in a higher overhead in terms of proportion of the required bandwidth. The testing at PNDC further indicates that the original message size is a significant factor influencing the security overhead as a percentage of the packet caused by applying the IPSec through a VPN. According to the test results, the employment of security will consume 22% to 28% of the total required bandwidth, as indicated in figure 2. It shows the estimated bandwidth requirement for the secondary substation RTU based on un-batched reporting (which results in the worst-case bandwidth requirements).

B. *TLS*

Another security level setup TLS, where a TLS certificate of the IP RTU is activated and managed through the connection. TLS is applied to enable authentication, encryption and data Integrity.

When TLS is applied, the captured packets get larger in size, especially during remote access testing. It is worth noting however that the large HTTPS packets will not be transmitted all times; they are only used during the remote access. This should be considered when identifying the bandwidth needed for activating remote access, (see Figure 2). The TLS application for remote access may be needed several times a month or even less. This means the bandwidth requirement is mainly affected by applying the IPsec to the packet with smaller size rather than the TLS packets.

Table 3 shows the impact of each protocol on the bandwidth, TLS authentication and the encryption along with the IPsec will require doubling the bandwidth used by the DNOs without security.

Not all applications will require two levels of security, i.e., device to device in addition to router to router, and overheads can be reduced if both are not used. However, DNOs have different approaches to identifying the level of security suitable for their organization. In many cases, this approach of relying on VPNs for location to location security combined with TLS for the end point devices makes deployment simpler.

The results are specific to tests configurations of one vendor's equipment, ascertaining the impact of the RTU and the configurations on the required bandwidth. This may require further testing and extending setup to include more vendors and a greater number of RTUs.

V. CONCLUSIONS AND RECOMMENDATIONS

Our results show that IPsec carries an average overhead of 25%, but this variable is highly dependent on the payload and configuration. Remote access communications tends to be bursty and bandwidth intensive. A good application response time is required for it to be effective. The overhead of TLS keep–alive messages, IPsec along with the TCP connections, and IEC 104 together consume more than 50% of the bandwidth (based on configuration and application). The security will add an overhead of roughly 2-3 fold of the existing data rate by the DNOs, for both levels of security (i.e. TLS and IPsec). The background traffic for security will add a significant overhead to the bandwidth.

The increasing use of IEDs and IT-based electric power assets increase the importance of cyber security in power utility. DNOs should consider smart grid security to include asset vulnerability, data management, data encryption, access control and data authentication, privacy concerns and threat profiling. Different data rates will apply to different DNOs based on their preferred configurations, communications technology types. Along with the number of set points and frequency of the measurements, they chose, and these are the main parameters affecting the required data rate.

A dedicated spectrum of 5 MHz is recommended to securely and remotely connect smart grid assets to the control centre and still cope with evolving LV applications. Private Network with such appropriate bandwidth and frequency band (i.e. low frequency spectrum bands for LTE 450 MHz) can tackle the main connectivity challenges for the smart grid in terms of rural coverage and required data rate. There is also a need for a common security approach or standard for the DNOs to be followed.

The next stage of our work will examine an IPSec VPN over different radio technologies (i.e. LTE-M band 3 or private/public LTE) and repeat the testing over different communication technologies using different vendors RTUs.

ACKNOWLEDGMENT

The authors acknowledge the contributions of Cisco, ABB, Scottish Power Energy Networks and other DNOs towards the successful completion of this PNDC research project.

REFERENCES

[1] K. McLaughlin, I. Friedberg, B. Kang, P. Maynard, S. Sezer, and G. McWilliams, “Secure Communications in Smart Grid: Networking and Protocols,” in Smart Grid Security, Elsevier, 2015, pp. 113–148.

[2] G. Research, “Trends in Utility Smart Grid Communications Management A GTM Research Whitepaper,” 2013.

[3] Ofcom, “Broadband and mobile coverage checker - Ofcom.” [Online]. Available: https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/advice/ofcom-checker. [Accessed: 19-Jan-2020].

[4] K. Ghanem, F. Coffele, and J. Irvine, “The reliability and optimal data usage of BGAN Satellite Communications for Remote Outstations,” in 2018 International Conference on Smart Applications, Communications and Networking, SmartNets 2018, 2018.

[5] R. Mcpherson, C. Hay, J. Irvine, and S. Member, “Using LoRaWAN Technology To Enhance Remote Power Network Monitoring,” 2019 IEEE 89th Veh. Technol. Conf., pp. 1–5, 2019.

[6] EU Directive 2016/1148, Concerning measures for a high common level of security of network and information systems across the Union', 6 July 2016

[7] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, “SCADA communication protocols: vulnerabilities, attacks and possible mitigations,” CSI Trans. ICT, vol. 1, no. 2, pp. 135–141, 2013.

[8] R. Mattioli and K. Moulinos, Communication network interdependencies in smart grids, European Union Agency For Network And Information Security, 2015

[9] “Engineering Recommendation G91 Issue 1 2012 Substation Black Start Resilience,” 2012.

[10] ENA, “Energy Delivery Systems-Cyber Security Procurement Guidance,” 2016.

[11] “Statement: Review of spectrum used by fixed wireless services - Ofcom.” [Online]. Available: https://www.ofcom.org.uk/consultations-and-statements/category-2/fixed-wireless-spectrum-strategy. [Accessed: 19-Jan-2020].

[12] D. and A. M. Group, “Allocation options for selected bands,” London, 2005.

[13] W. Wang and Z. Lu, “Survey Paper Cyber security in the Smart Grid: Survey and challenges q,” Computer Networks, vol. 57, pp. 1344–1371, 2013.