Bandwidth Efficient Secure Authentication and Encryption Techniques on IEC-60870-5-104 for Remote Outstations

[1]Kinan Ghanem
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
kinan.ghanem@strath.ac.uk

[3]Jidapa Hansawangkit
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
Jidapa.hansawangki@strath.ac.uk

[5]Rameez Asif
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
rameez.asif@strath.ac.uk

[2]Stephen Ugwuanyi
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

[4]Ross McPherson
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
ross.mcpherson@strath.ac.uk

[6]James Irvine
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—This work is based on the contributions and analysis from several ongoing technical projects and research activities of applying several security approaches in smart grid, namely, secondary substation of the future. The bandwidth requirements of Secure Authentication (SA), Transport Layer Security (TLS) and Internet Protocol Security (IPsec) encryption needed to secure future smart grid is presented along with a comparison between overheads from each security technique. Recommendations and discussions that cover the main challenges and prospects for the appropriate security approach for secondary substations are also presented.**

Keywords—Bandwidth, Encryption, IPsec, Remote Outstation, Secure Authentication, Smart Grid, Security, TLS

I. INTRODUCTION

As electrical grids transition into smart grids, reliable communication is required. This communication provides control and oversight of remote infrastructure. However, installing and securing these communication systems presents a number of challenges. Wireless networks reduce many of these challenges, and therefore present an efficient option for the power utilities to deploy. However, as the number of devices and their measurement resolution increases, so does the bandwidth required to operate these systems. This has financial and practical limitations for utility networks, as wireless systems require the use of a finite spectrum.

5G deployments offer a solution to this problem through a higher frequency spectrum. However, this may not be practical for utility networks with assets in rural or difficult to reach areas, where high frequency spectrum would struggle to permeate. Therefore, a sought-after low-frequency spectrum is required, which in turn grow the demand for the limited spectrum [1]. This necessitates the need to be conservative in bandwidth.

At the same time, encrypting and securing each connection in a smart grid is crucial. Mandatory requirements such as the Security of Networks & Information Systems (NIS) directive [2], dictate that critical national infrastructure such as utility networks must employ adequate security techniques. Simultaneously, future secondary substations automation systems will require a reliable communication solution to connect the distributed smart field devices to the management centre [3]. Thus, creating a requirement for secure, reliable and ubiquitous communication.

Commonly, the largest single providers of wireless networks are mobile network operators. These providers lease licensed spectrum in various bands and own thousands of masts providing wide geographical coverage. However, current generations of mobile networks provide between 99.50% (2 days downtime per year) and 99.92% (7 hours downtime per year). Compared to the energy regulators required 99.999% uptime (six minutes downtime per year). These more stringent requirements mean that most commercial wireless networks cannot support critical infrastructure.

This, therefore, may lead to the use of private or sliced mobile networks. Each of these would require dedicated spectrum allocations to ensure stable operation and smooth recovery from any potential black start scenario. Therefore, utility networks, mobile network operators and regulators are trying to identify the bandwidth and spectrum requirements to remotely monitor and safely operate distribution assets in future substations. This piece of work aims to clarify and assess the effects of vendors' configurations and communication media on the bandwidth and security requirements.

This work will further investigate the use of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) connection over radio technology (i.e. public LTE) using different vendors' Remote Terminal Units (RTUs) and various encryption techniques. Moreover, the project highlights the differences in the security bandwidth overhead needed between IPsec and TLS.

The key cyber security considerations in smart grid systems cover several technical areas such as IPsec tunnelling, TLS and secure authentication. This study is based on the IEC 60870-5-104 protocol for Supervisory Control and Data Acquisition (SCADA) systems to remotely monitor and safely operate distribution assets in substations of the future. The rest of this paper is organised as follows: Section II gives an overview and summary of related work. Section III presents a high-level overview of the security techniques used in the test. Sections IV and V then introduce the encryption test setup and the test results analysis, respectively. Next, Section VI presents a summary of the main encryption challenges for smart grids. Finally, Section VII concludes this paper.

This work was funded under the research programme of the University of Strathclyde's Power Networks Demonstration Centre (PNDC)

978-1-6654-3545-1/21/$31.00 ©20 IEEE

II. Related Work

Most existing communication channels currently used in the secondary substations are narrowband and limited [3]. New connected distributed assets such as charging points, Low Voltage (LV) monitoring and control, and renewable energy will further add more demands on the required bandwidth. Several research and studies have been accomplished to investigate the cost of security in smart grid applications. However, there are limited practical investigations on deploying TLS encryption in the secondary substations [4] [3] [5]. A TESLA authentication mechanism has been considered to secure communication between smart grid systems and distributed smart meters gathering energy consumption data [6]. A novel smart meter authentication scheme as proposed in [7] secured smart grid communication based on Verifiable Random Function (VRF) using Elliptic Curve Cryptography (ECC). In [8], a revision for DNP3-SA module to eliminate bandwidth overhead is proposed. However, research which covers the encryption for IEC 104 in secondary substations of the future is very limited, and few are survey studies presented in Table 1.

Table 1. Summary of Related Literature and their contributions

Authors	Year	Reviewed area and contribution
Yuan et al. [9]	2021	A lightweight and communication efficient data aggregation scheme for smart grid systems is proposed. The proposed approach aimed to reduce the complexity and computation costs of the traditional scheme.
Narayana [10]	2012	Various security threats at each OSI layer identified with an overview of layer 2 security standards such as 802.1AE and 802.1X presented.
Ghanem et al. [3]	2020	Presented a use case involving the trial of a solid-state transformer which provides flexibility and security functions for the smart grid.
Hiller et al. [11]	2019	Analysed the impact of TLS on clients and servers and proposed a protocol compatible redesign of TLS session management to be used in different mobile data applications.
Rosborough et al. [12]	2019	Introduces security protocols used in ICS environments for DNP3 protocol.
Yuanyuan et al. [13]	2008	Analysed the security requirements of data communication in wind power farms and provided recommendations for improving TLS protocol to strengthen the security of renewable energy sources.

III. Security for secondary substation

Various security techniques are used in power utilities for authentication, management, encryption and certificate updates purposes [14]. For example, IPsec authentication and encapsulation standards are widely used to establish secure VPN connections [1]. IPsec protocol is considered in the bandwidth calculations as a level of security when using a Wide Area Network (WAN). Moreover, TLS, Hypertext Transfer Protocol Secure (HTTPS), File Transfer Secure Protocol (FTSP) and Simple Network Management Protocol (SNMP) are also applied to secure connections in smart grid. As part of the project, various workshops were conducted at the University of Strathclyde Power Networks Demonstration Centre (PDNC), involving utility operators, mobile operators, regulators, policy makers and technology vendors to ascertain the security requirements for smart grid applications.

Future electrical power systems require an upgrade that is more resilient, secure, and efficient technology to improve capacity and reliability with increased automation [15]. Previous research discovered that existing secondary substations where several communication technologies are already deployed without adequate security. The key security recommendations and directives according to our technical discussions are to use secure communication technologies to prevent cyber-attacks. This implies that in remote outstations, securing the distributed assets and ensuring that field measurements are transmitted securely should comply with the security standards for power utility (i.e. IEC62351, IEC62443/ISO27001 and ENA Security Procurement [10]). Secondary substations of the future will include more functionalities to perform additional monitoring, reporting and control capabilities. The communication needed to enable that should be highly secured. However, one concern in securing this communication is the acquisition of the bandwidth required.

Cryptographic methods such as VPNs, wrappers (in the form of TLS), and protocol security extensions are three common methods of implementing cryptographic concepts in distribution networks [16]. While TLS aims to secure the communication channel between the end devices and the control centre, IPsec provides security through a VPN tunnel between routers. IPsec provides robust authentication, integrity verification and sufficient encryption to the traffic. TLS does not initiate a tunnel; it encrypts the application level data. The protocol security extension such as Distributed Network Protocol 3 Secure Authentication (DNP3-SA) aims to authenticate the end devices and ensure the message integrity between the master and the filed device [12] - [17].

Another point to note is the need to remotely access the field device, which will require a secure end to end connection through a trusted VPN tunnel to perform any required configurations and maintenance. The VPN will encrypt the network connection and could allow the power networks to provide secure connectivity between their remote devices over a third party network, as the transferred data via any protocols should be encrypted and authenticated. For instance, establishing an encrypted tunnel, the procedures of encryption and authentication at both IPsec tunnel ends must match. This can be done via sharing a key to the encryption code.

A. TLS encryption

Transport Layer Security (TLS) is used in the industry for end-to-end encryption as it plays a significant role in several existing applications. However, many challenges identified in this study should be observed before TLS is deployed in the utility sector. They include using a unique certificate for each device, with unique public and private key, and ensuring TLS sessions certificate update. TLS is supported by different utility protocols such as IEC 60870-5-104 employed in this study. Similarly, several vendors RTUs such as Virtual Access and ABB also support TLS in their field outstations and gateways. A public key certificate signed by a trusted certification authority containing secure Cipher Suites that offer at least 128-bit encryption keys is needed to comply

with the NIST recommendations [15]- [17].

TLS encryption for both DNP3 and IEC 60870-5-104 communication can be enabled in the RTU to secure the exchange of data between the control centre and the RTU. Also, configuring the IEC 60870-5-104/DNP3 master to use TLS is also required. IEC 62351 standard recommends updating the Session Key at least once in 24 hours. TLS handshake aims to authenticate the end connected devices and ensure successful exchanging of the cipher suites, symmetric session keys and parameters between the client and the server prior to any communication between the end parties. Once the entire TLS Handshake is successfully completed and the peers validated, the applications on the peers can begin communicating with each other.

B. Secure Authentication

In order to help the power utilities improve the security of their networks, a Secure Authentication (SA) approach is presented. It is derived from IEC 62351 and applies to a range of protocols such as IEC 60870-5-101, IEC 60870-5-104, and IEC 61850. When activating the SA in SCADA systems, each critical message requires authentication before any execution. As messages can be authenticated with a procedure called challenge/reply shown in Figure 1. DNP3 SA v5 (i.e., IEEE 1815-2012) enables the DNP3 master to include the Hash-based Message Authentication Code (HMAC) in its original transmitted DNP3 message. Including the necessary authentication data in the original message can reduce the bandwidth needed as fewer messages are transmitted [18]. The test setup, which uses SCADA gateway from Virtual Access, supports SA as defined in the IEC 60870-5-7 standard.

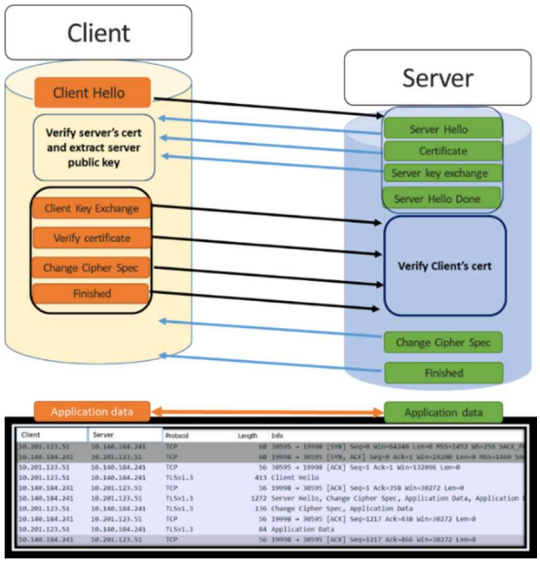

Figure 1 Handshake main authentication and key messages exchanged

Adding authentication - based on IEC 62351 security standard to an existing SCADA protocol ensures that any critical commands are safe and may avoid any possibility of a man-in-the-middle attack that will affect the connection. The main advantages are the ability to support low bandwidth and serial networks for legacy equipment such as IEC 60870-5-101, and create low overhead for remote outstations that may not be capable of processing any public/private certificates or encryption. Due to several limitations and restrictions, many existing Operational Technology (OT) protocols and devices may not have any security such as authentication and confidentiality. The limited available channel to add any security to the existing technology makes it more difficult for the power utility to deploy security. Recently, many energy networks started to include security in their protocols, especially those designed by the IEC group. Where, for some legacy protocols and applications, TLS and IPsec may not be able to provide end-to-end encryption, and identity management, the only choice becomes the SA. This could open the door to the importance of lightweight encryption approaches which can be used in such constrained environments.

In computationally constrained environments, new lightweight encryption standards are required to execute asymmetric cryptography. The international cryptographic competition which is organised by NIST and expected to be completed this year, will open the door for more encryption research communities and industry stakeholders to evaluate and select widely efficient, cost-effective, lightweight algorithms [19]. It is expected that an extensive analysis and performance benchmarking will be conducted and based on the findings recommend a new lightweight encryption standard to NIST's portfolio. This could be used by utilities to provide end-to-end encryption and identity management as a projected option to be used in a limited environment in terms of bandwidth and resources. Moreover, lightweight encryption algorithms are a way out of the OT security protocol issues in terms of the absence of authentication and confidentiality in certain applications.

IV. ENCRYPTION TEST SETUP

To estimate the bandwidth requirements for the remote outstation, different communication nodes have been chosen to enable the right connectivity on the SCADA software needed to control the filed devices and poll for measurements. This is practically the control system polling the RTU through an industrial SCADA protocol to enable the connectivity between the RTU and control centre. A high level diagram of the test setup is shown in Figure 2. Triangle MicroWorks, two industrial routers and gateway, and two 4G LTE sim cards were used to establish the connectivity needed to test the encryption techniques. The chosen gateways which support secure authentication, TLS and IPsec were used in all the test setups and experimental scenarios.

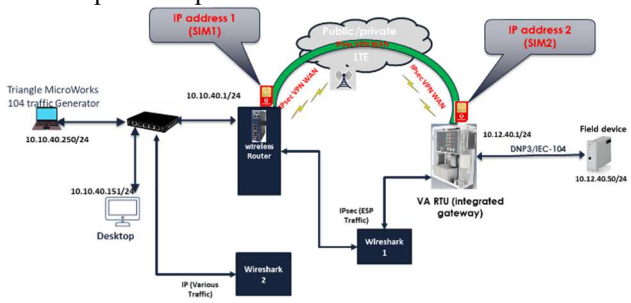

Figure 2 High-level Initial Test Setup for TLS encryption

The protocol used to link the RTU with the SCADA control centre is the IEC 60870-5-104 (IEC-104) which is

generated from the Triangle MicroWorks traffic simulator. The tests configuration scenarios were chosen based on the discussion with several power networks operators as a trail to reflect the real status of their existing network configurations. The main IEC-104 commands were based on several digital and analogue commands which are used for SCADA polling in this test. The main digital commands were: general integration, counter integration, single point, and double point. The analogue commands were: normalised measured, scaled measured, floating measured, Clock synchronisation and 32-Bit string. The same configurations have been repeated for each security approach, aiming to understand the overhead caused by each security approach.

V. Test Result Analysis

In the test phase, we considered different test setups with various security techniques over the same configurations in IEC 60870-5-104 (IEC 104) protocol. The methodology used in this work is completely based on the captured data from the Wireshark network analyser. Each test scenario is analysed to identify the unique packet size, which in turn is scaled and used to estimate the monthly data usage needed by an RTU.

A. Secure Authentication Overhead

The main observation from activating the secure authentication approach is that the Message Authentication Code (MAC) is used to authenticate the critical command using session keys. MAC could double the bandwidth for some configurations (for a high number of polls in order of seconds) because the authentication requires a challenge/reply procedure for each command. For the same configurations with a limited number of commands each in minutes, every setup ran over a specified time, and the data usage needed for the dedicated test time calculated and analysed before the obtained data usage was scaled and extended to cover the cost over a month. The estimated monthly data without any security is 49.3 Mbyte, whereas the overhead caused by the authentication using IEC-104 is about 55 Mbyte a month. The estimated security overhead for reply/challenge authentication is less than 10 % of bandwidth, and the maximum data rates did not exceed 7% of the existing data rate needed in bps, as shown in Figure 3 and Figure 4.

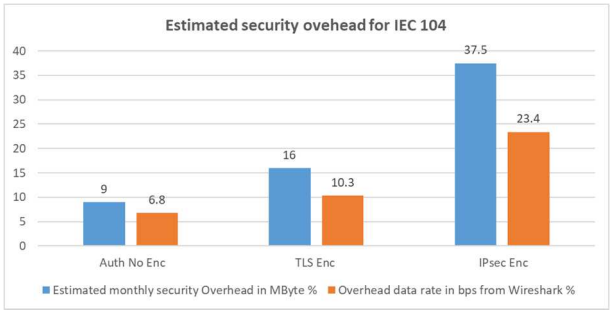

Figure 3 Estimated overhead for different security approaches

In secondary substation applications where the frequency of the critical commands is limited, the authentication could be used to ensure that the control centre is talking to an authenticated field device. This option is applicable mainly when there is a restriction in the available bandwidth for the remote outstation. Authentication proves that a message was sent by the right device, as it allows the sending device to confirm other device IDs, unlike encryption which hides contents of a message and is only read by the destination device.

It is important to mention that secure authentication supports the legacy, serial protocol, a feature that makes it suitable to work in low bandwidth conditions (i.e., it creates low overhead for remote outstations that may not be capable of processing any existing encryption such as TLS or IPsec as it will be illustrated in the next subsections).

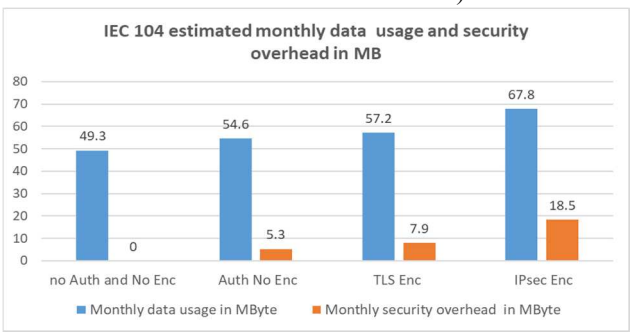

Figure 4 Estimated monthly data usage for different security approaches

B. TLS vs IPSec Overhead

As shown in Figure 1, the TLS session negotiation begins with handshake messages between the control centre and the outstation device. After successfully authenticating and exchanging messages between the client and the server, a change cipher specification (spec) message is exchanged between the master SCADA and the RTUs identifying that the communication is encrypted. The estimated overhead to establish a new TLS session is between an average of 3-6 Kbytes (based on the certificate size) for a certificate size of 2048 bits. On the other hand, the estimated overhead to resume an existing TLS session comes to about 330 bytes on average. However, the estimated overhead of the encrypted data using AES-128 as a block cipher is 22 bytes for each captured packet/frame (25% of the overhead needed for each packet encrypted by IPsec). The above results may vary if there are changes in the configurations and running traffic pattern.

Therefore, the establishment of an encrypted TLS communication session requires an average of 4.5 Kbyte (subject to the certificate and key size) to be exchanged. As the frequency of the handshake increases, so does the bandwidth. In a constrained environment with limited resources and inadequate available data rates for each RTU, this can take more time and waste the limited available resources. For example, in the black start scenario, this can create a delay in establishing the end-to-end secure encryption session and further delay bringing back the grid to normal operation.

In scenarios where the majority of the exchanged messages between the SCADA and the RTU are less than 100 bytes, the estimated average TLS overhead with AES-128 key is 16% for each packet. If setups have larger packets size,

the percentage security overhead for each packet would decrease. Adding TLS encryption with SHA-256 will attach 32 bytes for each packet whereas IPsec will almost add double that for each packet when using IPsec. An overhead of around (11-17) % for the original monthly bandwidth needed in Mbyte without encryption is observed when applying TLS encryption. The estimated monthly overhead for using TLS with AES-128 contributed around 8 Mbyte a month for the existing bandwidth needed to run one RTU as shown in Table 2.

TLS does not encrypt the TCP packet unlike IPsec which encapsulates all the packets inside the tunnel. TLS traffic could compose an average of 40% of the total exchanged traffic based on the analysis from the test setup. While the majority of TCP packets sizes are smaller than the IEC-104 packet size, the security overhead contributed by the TLS will be smaller than the IPsec. As IPsec will add an average of 60 to 68 Bytes for each packet that enters the IPsec VPN tunnel. Field devices need to download the certificate revocation list to ensure that the exchanged certificate is valid and trusted. TLS certificates length vary between 1024 to 4096 bits and it is an important requirement for estimating overhead associated with the session and handshake messages exchange. Certificates of 2048-bit length fulfil the NIST certificate recommendations, X.509 certificate with 2048-bit public key is used in our test. TLS as we found is a secure option for critical applications, as it uses certificates for all connected devices and can encrypt the data of any chosen application.

VI. ENCRYPTION CHALLENGES IN SMART GRID

The recommended encryption techniques for the smart grid vary and depend on the power network architecture, the deployed communication technology and the end application. Although secure authentication might be used in limited resources and legacy devices, it does not encrypt the exchanged data. Both IPsec and TLS provide security by encrypting the exchanged messages. TLS encrypts the data from the control center to the end device, whereas, IPsec is encrypts the data through the tunnel between the two end routers. TLS can be implemented easily to encrypt, authenticate, and also check data integrity. It can be further employed to secure other applications and protocols including VoIP and web-based applications.

Table 2 The Estimated Overhead needed for Different Security Approaches using IEC 104

IEC 60870-5-104	IEC 104 with Authentication	IEC 104 with TLS	IEC 104 with IPsec
Monthly data usage MByte	54.6	57.2	67.8
Monthly security overhead MByte	5.3	7.9	18.5
Monthly security overhead in %	9 %	16 %	37.5 %
Overhead data rate in bps from Wireshark %	6.8 %	10.3 %	23.4 %

From the bandwidth point of view, TLS is more bandwidth efficient and would require less bandwidth than IPSec. As shown in Table 2, although the monthly cost of TLS encryption is less than the monthly cost needed in IPsec, TLS in the black start scenario contributed an additional 40% of the overhead needed to restore the service. Inputs from the knowledge exchange discussions indicate that power network operators prefer to completely rely on their network and avoid (if possible) third party support. The IPSec approach which might be relied on a secure tunnel owned by third parties may be considered an alternative without a private network. For the secondary substation of the future, where the substation could be the main interface and the essential gateway for RTUs and LV applications, the availability of reliable network connection with adequate bandwidth will continue to be the bottleneck. For network connectivity provided by a third party where RTUs and gateways can be fitted with appropriate roaming sim cards (multi-network sim cards). When a network issue is detected in one mobile network operator's service, the devices can automatically move onto another provider, offering increased redundancy. The architecture of existing public mobile networks prohibits direct device to device connections therefore, all connections have to go through an intermediary. If this service was to fail, so would the device connection. The lack of control and influence of the third-party network could create high network interruption during a blackout. Private mobile network or networks employing control and user plane separation with a local user plane function can enable direct device to device connectivity.

Poor network coverage and congestion increases the number of dropped packets and degrades the system performance. The reliability in terms of packet loss and retransmission rate is highly affected by the quality of the communication medium (coverage and signal quality). Based on the encryption tests conducted at the PNDC, the secure tunnel shows high reliability over most scenarios. The multi-sim card which can pick the best available signal among several Mobile Network Operators (MNOs) increases the reliability of the connection. On the other hand, using multi-network sims from a third party provider could disturb the connection and cause the tunnel to fail in case of any problem with the third party servers. We observed that the quality of the communication medium can affect the reliability in terms of packet loss and retransmission rates. Several clarifications that might affect the reliability of the connection as obtained are listed below:

- Connection failure due to power and radio signal loss will result in the loss of TLS or IPsec tunnels providing secure data and command exchanging path for the field device.
- Network congestion, configuration error and lost packets could affect the reliability especially when a third-party service provider is involved.
- Synchronisation problems between the master clock and field devices could drop the reliability. Network delay can lead the authentication to fail.
- The length of the encryption key, AES with length 256-bit key and more will consume more bandwidth and will require high-end processing capabilities which may not be found in all gateway field devices. This could significantly affect the reliability and

increase packet loss. AES of 128-bit key size is NIST recommended for lightweight encryption.

VII. Conclusion

This paper discussed secure authentication and compared the security overhead of TLS and IPSec encryption for smart grid remote outstations. This fulfils the lightweight security requirements of the smart grid in connecting distributed smart grid assets to the control centre remotely. In power utility where reliability is the highest priority in OT environment, we found that secure authentication is a cost-effective solution in a constrained asset, incapable of supporting encrypted protocols such as TLS or IPsec. TLS with AES-128-bit key size contributed only 25% of additional overhead when compared to IPsec for each analogue or digital command. The main recommendation for the study found that one level of security will be sufficient for remote outstations, as less than 100 Mbyte a month can easily fit with the security requirement for each sim card needed to securely connect an RTU.

The optimal data usage of proper wireless communication technology for remote outstation is best obtained by choosing the correct test configurations, in addition to the appropriate security technique needed to secure the connection. Multi-networks sim card which can pick the best available mobile signal (from different operators) increases the reliability of the connection in terms of packets loss and retransmission rate. Future work will look at testing different protocols such as IEC 61850 and DNP3 over different end applications and various secuirty techniques.

Acknowledgment

The authors acknowledge the contributions of PNDC members (mainly, Scottish Power Energy Networks, Scottish and Southern Electricity Networks, UK power networks, Vodafone and Virtual Access) for their valuable discussions over different meetings and knowledge exchange forums. Special thanks to Artur Wachowski from Virtual Access for his support during the project test period.

References

[1] K. Ghanem, R. Asif, S. Ugwuanyi and J. Irvine, "Bandwidth and Security Requirements for Smart Grid," in *IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020.

[2] NCSC, "NCSC CAF guidance," National Cyber Security Centre (NCSC), 30 September 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/caf. [Accessed 07 May 2021].

[3] K. Ghanem, I. Abdulhadi, A. Kazerooni and C. McGookin, "Communication requirements for future secondary substations to enable DSO functions," in *CIRED Workshop 2020. 2020*, Berlin, 2020.

[4] P. Urien and M. Estelle , "Securing the IoT with TLS/DTLS server stacks embedded in secure elements: An ePlug usecase," in *14th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 569-570. IEEE, 2017.*, 2017.

[5] S. Lakshminarayanan, "Authentication and authorization for Smart Grid application interfaces," in *2011 IEEE/PES Power Systems Conference and Exposition*, Phoenix, 2011.

[6] D. Inshil , . L. Jiyoung and C. Kijoon , "Secure Authentication for Structured Smart Grid System," in *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Santa Catarina, 2015.

[7] B. Pranali , M. Bharati and J. Debasish , "A Novel Smart Meter Authentication Scheme for Secure Smart Grid Communication," in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, Kochi, 2019.

[8] C. Mumin and A. Kemal , "A Bandwidth-Efficient Secure Authentication Module for Smart Grid DNP3 Protocol," in *2020 Resilience Week (RWS)*, Salt Lake City, 2020.

[9] Y. Su, L. Yanping , L. Jiliang and K. Zhang, "LCEDA: Lightweight and Communication Efficient Data Aggregation Scheme for Smart Grid," *IEEE Internet of Things Journal,* no. 2327-4662, 2021.

[10] N. R. Indukuri, "Layer 2 security for Smart Grid networks," in *IEEE International Conference on Advanced Networks and Telecommunciations Systems (ANTS)*, Bangalore, 2012.

[11] J. Hiller, M. Henze, T. Zimmermann and O. Hohlfeld, "The Case for Session Sharing: Relieving Clients from TLS Handshake Overheads," in *2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium) (PP. 83-91).*, Osnabrueck, 2019.

[12] C. Rosborough, E. C. Gordon and B. Waldron, "All about eve: Comparing dnp3 secure authentication with standard security technologies for scada communications," Schweitzer Engineering Laboratories, Inc, 2019.

[13] L. Yuanyuan and D. Bin , "Strengthen the security of data communication in wind power farm with improved TLS protocol," in *2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*, Nanjing, 2008.

[14] S. Ugwuanyi and J. Irvine, "Security Analysis of IoT Networks and Platforms," in *International Symposium on Networks, Computers and Communications (ISNCC)*, Montreal, QC, Canada, 2020.

[15] M. I. Henderson, D. Novosel and L. M. Crow, "Electric power grid modernization trends, challenges, and opportunities.," IEEE, 2017.

[16] C. Rosborough, "All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications," Exelon and Schweitzer Engineering Laboratories, Inc., Washington , 2019.

[17] R. S. Geetha, S. Gowdhamkumar and S. Jambulingam, "Energy challenge, power electronics & systems (PEAS) technology and grid modernization," *International Research Journal of Multidisciplinary Technovation,* vol. 1, no. 2, pp. 116-129, 2019.

[18] F. Cleveland, "IEC TC57 security standards for the power system's information infrastructure–beyond simple encryption," in *Transmission and Distribution Conference and Exhibition,* , 2005.

[19] M. S. Turan, "Lightweight Crypto, Heavyweight Protection," NIST, 13 01 2021. [Online]. Available: https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection. [Accessed 07 05 2021].

[20] C. C. Sun, A. Hahn and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018.