Mobile Secure Communications in Smart Grid Control

Giovanna Dondossola and Roberta Terruggia(✉)

Transmission and Distribution Technologies Department,
Ricerca sul Sistema Energetico, Milan, Italy
{giovanna.dondossola,roberta.terruggia}@rse-web.it

Abstract. This paper analyses the communication required to connect the Distributed Energy Resources with power grid substations securely. The IEC 61850 standard communications enhanced with IEC 62351 security standard are evaluated by implementing the information exchanges related to voltage control in an experimental test bed deploying cellular M2M access networks. Particularly the end-to-end security is implemented using peer authentication and packet encryption in compliance with the IEC 62351-3 standard profile. Based on the network traces obtained from the test bed, the security overhead and the impact of cellular networks on transmission delay are measured by protocol specific performance indicators and the results are discussed in the paper.

Keywords: Cellular networks · Cyber security · Distributed energy resources · Standard communications · Voltage control

1 Introduction

The probability of security threats to critical infrastructures of smart grids has been increasing with the deployment of advanced automation and communication technologies, specifically considering the connection of DER (Distributed Energy Resources) from third parties with the power grid substations located in the DSO (Distribution System Operator) domain. Given the high severity of possible communication malfunctions, stringent time and security requirements have to be meet by DER control communications, with a major focus on *deterministic transmission delays* of monitoring and control data exchanges, *high availability* of always on communication links, *no losses* of application messages, *authenticity and integrity* of sending and receiving data streams. The achievement of such challenging requirements using standard communications for interoperability purposes and telecommunication services based on new generation cellular M2M technologies for economic convenience is an ambitious objective for the roll out of full smart grids. Of great importance for the technological evolution of smart grids is the setup of experimental platforms for the performance evaluation of the entire communication architecture and the definition of measurable performance indicators as part of the service level agreement with the telecommunication provider. The experimental activity described in the paper is exactly meant to address such an urgent need.

E.T. Lau et al. (Eds.): SmartGIFT 2017, LNICST 203, pp. 182–191, 2017.
DOI: 10.1007/978-3-319-61813-5_18

In this paper the focus is on the security of the communications among the DERs and DSO substations.

Section 2 introduces the related work on SCADA (Supervision Control And Data Acquisition) systems and communications between Substations and DERs, the communication standard IEC 61850 and the security standard IEC 62351, and the cellular access network. Section 3 details the reference voltage control use case and explains the setup and configuration of an experimental test bed implementing the IEC 62351-3 compliant security enhancement of the use case communications over the mobile M2M network. The evaluated metrics and results are compared and discussed in Sect. 4, followed by the conclusions and future works in Sect. 5.

2 Background

The traditional SCADA systems need to be enhanced in order to allow the Smart Grid control. More in specific SCADA infrastructures require to support the management and operation of the MV grids in DSO control centres and substations in this new landscape. To integrate with active DERs connected to MV bars and feeders, the architectures of current SCADA systems have to be upgraded with new control functions and related information exchanges. In [1] an ICT architecture is described detailing the information flows required by the voltage and power optimization algorithm as defined in [2].

2.1 IEC 61850 – MMS

IEC 61850 defines standardized data models, communication services and protocol profiles for the information exchanges in substations based on both state of the art communication technology and powerful object modelling. The approach of IEC 61850 is based on the separation between the object models virtualizing real devices and their components and the requirements on the underlying communication protocols, in order to be technology independent and hence “future-proof”. The object models are defined in terms of standardized types and services. Real devices and functions are modelled by Logical Nodes composed by standardized data objects. Logical Nodes are grouped into Logical Devices which model the behavior of Intelligent Electronic Devices (IED). The abstract definitions provided by IEC 61850-7 are independent of specific protocol stacks, implementations and operating systems. IEC 61850-8-1 [3] specifies how to implement the services and algorithms defined in IEC 61850-7 by using the MMS (Manufacturing Message Specification) [4] and other protocols. Object models modeling DER systems are defined in IEC 61850-7-420 [5] which is under development as a DER specific part of IEC 61850 standards.

2.2 IEC 62351

The scope of the IEC 62351 series is information security for power system control operations. Its primary objective is to undertake the development of standards for security of the communication protocols defined by IEC Technical Committee 57 for the information exchanges in power systems. According to the security standard IEC 62351-3 [6], the SCADA and telecontrol protocols that make use of TCP/IP as message transport layer have to be protected by specific TLS (Transport Layer Security) configurations applicable to the telecontrol environment. Specifically securing the MMS traffic via IEC 62351-4 and IEC 62351-6 is done on the application and the transport level. Message authentication is performed at the application level by carrying authentication information in the protocol data units. Authentication information comprises a X.509 encoded certificate, a time stamp and the digitally signed time value. For security on the transport layer IEC 62351 refer to TLS [7]. The document specifies the use of port 3782 for secure communications instead of standard port 102. It also specifies a set of mandatory and recommended cipher suites (the allowed combination of authentication, integrity protection and encryption algorithms) and states requirements to the certificates to be used in conjunction with TLS. These requirements comprise for instance dedicated certificate context, application of signatures, and the definition of certificate revocation procedures.

2.3 Cellular M2M Networks

Due to the different penetration of the communication technologies in the geographical regions where DER sites are located, the control functionalities shall work with heterogeneous DER networks (e.g., wired, wireless). The communication can be carried by different cellular technologies, in particular the new generation of cellular networks uses technologies, like LTE and LTE-Advanced, which theoretically meet the most stringent requirements for higher data rates and lower latencies of the most demanding smart grid applications [8].

3 Experiment Setup

This section presents the implementation in a laboratory environment of a platform for the analysis of the communications needed by the Medium Voltage Control function.

3.1 Use Case – Voltage Control in Active Grids

The connection of DERs to medium voltage grids can influence the state of the power grid, affecting the capacity of the DSO to comply with the terms contracted with the TSO (Transmission System Operator) and can have an impact on the quality of service of their neighbor grids. In order to maintain stable voltages in the distribution grids a Voltage Control (VC) function has been designed [2] to monitor the grid status acquiring field measurements and to compute optimized set points for the available flexible assets such as DERs, flexible loads and power equipment deployed in HV/MV substations. The VC function is performed by a controller that is a node of a HV/MV substation control network. In order to compute an optimized voltage profile, the algorithm needs to communicate both with components inside the DSO area, and with systems outside the DSO domain. In particular DERs and flexible loads communicate with the controller via the DER/Flexible loads communication network, possibly deploying heterogeneous communication technologies. The system level outlay of the voltage control function is shown in Fig. 1. Its detailed specification can be found in the Annex B of [1].

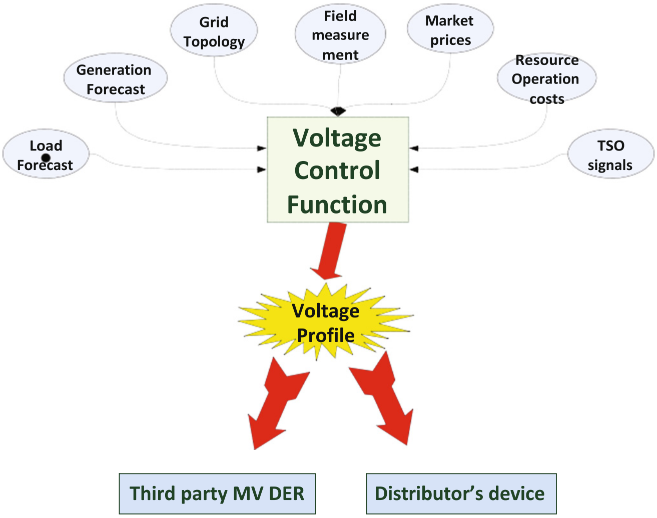

Fig. 1. Voltage control function

3.2 Test Bed Layout

A test platform has been set up in RSE PCS-ResTest Lab (Power Control Systems – Resilience Testing Laboratory) [11] for running cyber security experiments over realistic VC scenarios in the operation of active grids. Figure 2 illustrates the simplified view of the physical setup deployed for the experimental analysis [12]. At the logical level the test bed consists of a set of software building blocks including in particular for the focus of this paper:

- **HV/MV substation network:** each substation includes automation, communication, SCADA and Operator HMI functions. At each substation the behavior of the electrical process is simulated by a Field Simulator application that cyclically reads and updates a virtual I/O interface. The substation hosts the client module managing substation-DER communications.
- **DER sites:** 4 large DERs sites connected to the HV/MV substation through the server module.
- **DER control networks:** connecting each DSO substation with multiple third party DER sites located in different geographical areas deploying heterogeneous communication technologies.

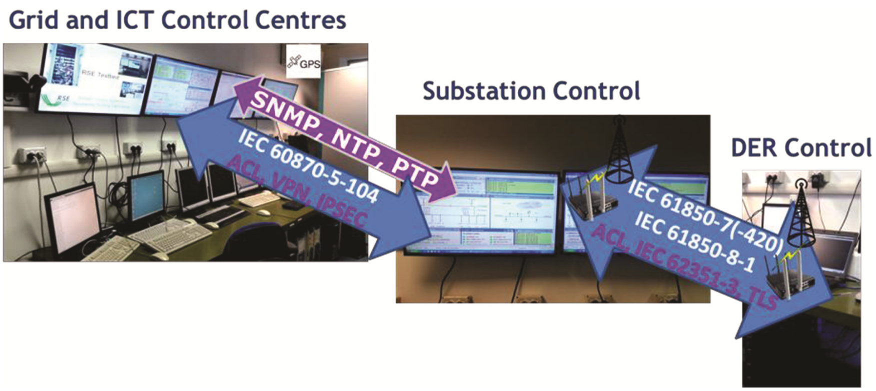

Fig. 2. Test bed layout

3.3 M2M (Machine to Machine) Cellular Network Configuration

In order to evaluate the performance of cellular M2M network technologies (e.g., LTE/4G, 3G and 2G) that enable the connection of DER sites with the DSO substations, one DER site in our test bed is connected to the substation through a wired Ethernet VLAN (Virtual Local Area Network) as the baseline test, and three DER sites (located in the RSE test facility and in other places in the Milan area) are connected via a cellular network. Data from substation and DER move in and out being routed through the M2M LTE network, by proper LTE SIM cards inside 4G routers configured with private static IP addresses. Both the primary substation and the DER rely on their own Ethernet based LAN, and connect to the mobile access network via LTE routers, through a GRE (Generic Routing Encapsulation) tunnel configured on both sides.

3.4 Client and Server Test Application Based on IEC 61850

MMS information exchange between DERs and substations, related to the VC scenarios, is provided by a test client-server application: the server application is associated to the DER site while the client resides on the substation SCADA. The client establishes an MMS session with the server, requests the transmission of the IED’s profile (as specified by IEC61850), then enables a report control block provided by the server requiring the transmission of periodical information reports. The number of reports to be sent by the server and the interval between the emission of two consecutive reports are configurable. Report transmission causes the information flow from the server towards the client. To generate the information flow in the other direction, from the client towards the server the test client can be instructed by the user, to send setpoints on a periodic basis. Also in this case the period is configurable. The client-server application is implemented on top of the API provided by the libIEC61850 library [9]. In turn the library implements the most important parts of IEC 61850 on top of the MMS mapping, providing the MMS services needed by IEC 61850.

3.5 Security Features According to IEC 62351-3

Security features as specified by IEC 62351-3 have been integrated into the communication protocol by enabling TLS encryption and authentication as stated in the security standards for TCP/IP based protocols, specifically MMS. The implementation of the TLS protocol is based on OpenSSL [10].

As mentioned before the MMS protocol stack is implemented by libIEC61850. This library provides a Hardware/OS Abstraction Layer (HAL) to hide the dependencies from the underlying platform. Currently this layer consists of thread, socket and time abstractions. To support TLS enabled sockets, a TLS HAL implementation for POSIX (Linux) is added to the library, which is shown in Fig. 3. The TLS HAL module works as a wrapper offering the library's standard socket API to the upper layers but providing TLS authentication and encryption services. The TLS extension is transparent to the upper layers of the MMS application: the adoption of TLS protection for MMS traffic does not cause any change to the application. To establish a TLS session on top of a TCP connection, the TLS HAL uses the OpenSSL library, which is a free (BSD-style license) C implementation of SSL/TLS based on Eric Young's SSLeay package. Server side listens on secure port (3782) and supports basic authentication, encryption and message authentication according to TLS v1.2 [7].

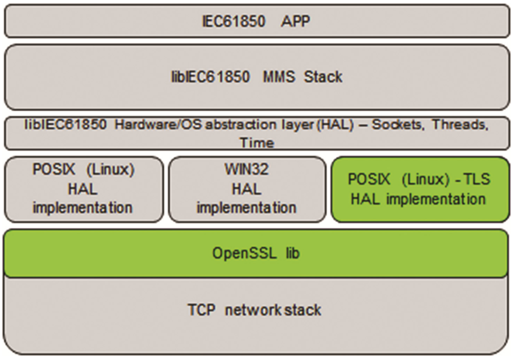
IEC61850 APP
libIEC61850 MMS Stack
libIEC61850 Hardware/OS abstraction layer (HAL) – Sockets, Threads, Time
POSIX (Linux) HAL implementation
WIN32 HAL implementation
POSIX (Linux) - TLS HAL implementation
OpenSSL lib
TCP network stack

Fig. 3. libIEC61850 MMS stack and IEC 62351-3 implementation

3.6 Test Cases

The medium voltage control test bed focusses on the core control and communication components for the voltage control use case. Also the components supporting ICT maintenance and monitoring functions are integrated in the test bed. Up to now, the tests carried out on our test bed as described in the above sections, can be grouped into two comparable test classes verifying the behavior of communication under the following security measures:

- **Plain Security:** tests verifying the VC communications with basic security measures, i.e. access control to communication gateways. These tests aim at checking the plain communications among DSO substations and DER sites. Both Ethernet and cellular

technologies are tested to be compared with each other according to several performance criteria.
- **Standard Security:** tests verifying the VC communications with enhanced security measures as suggested by IEC 62351 Part 4 in T-Profile (currently including TLS profile recommended by IEC 62351-3).

4 Methods and Results

In order to stress the various aspects of the protocols involved, two scenarios have been setup:

- **Short tests:** repeated runs (i.e. 10 runs) of relatively short test (50 reports sent from MMS server and setpoints sent from MMS client);
- **Long tests:** a single run of MMS where thousand (i.e. 2000/50000) of reports and setpoints are emitted by the MMS server and setpoints by the MMS client respectively;

These different scenarios are used in order to obtain relevant estimation of the metrics described in the next subsection. The first scenario is used to evaluate the mean time of the indicators related to the handshake and session setup, the second one provides report and setpoints statistics.

4.1 Metrics

The traces achieved during the test session have been analyzed through a customer built tool that it is able to extract and calculate several interesting indicators. In particular the trace analyser is used to obtain the values of the following performance indicators:

- TCP/TLS Handshake Time: handshake duration for TCP connection/TLS session.
- TLS renegotiation/resumption Time: the time required for renegotiation/resumption operations.
- MMS handshake Time: the time required for the establishment of the MMS session.
- MMS Profile Exchange Time: the exchange duration of the MMS profile between client and server.
- RTT (Round Trip Time)-Report: the time interval between the output of a report and the reception of the corresponding TCP acknowledgment by the MMS server.
- RTT-Setpoint: the time interval between the output of a setpoint request and the reception of the corresponding TCP acknowledgment by the MMS client.
- Inter-Report Time or Inter-Setpoint Time: the time interval between each two consecutive reports or setpoints, respectively.
- Number of TCP Retransmissions for a report or a setpoint.

The Standard Security test trace analysis required a way to perform the deep packet inspection. This is an issue currently under discussion within the IEC TC 57 WG 15 committee and until now a standard solution doesn’t exist. In our tool the problem has been worked around and messages are decrypted knowing the server private key and the data exchange during the TLS session handshake.

4.2 Results and Discussion

Table 1 lists the average values for time metrics, e.g. TCP/TLS handshake time, MMS profile exchange time or RTT-Report etc., for the test scenarios. The values are extracted from the two test groups. Short tests provide the best approximation for the metrics considering handshake and session/profile exchange because in these tests we have different runs. Long tests have been used to estimate Renegotiation time, RTT-Setpoint and RTT-Report thanks to the thousands of reports and setpoints included in the test. The packet size has a strong impact on the time value of the indicators. In particular the profile size influence the handshake times. The profile size is 2914 byte, the report packet size is 230 (259 with TLS)

Table 1. Metrics for test scenarios

Test case	Network	Metrics (time in seconds)								
		TCP handshake time	TLS handshake time	TLS renegotiation time	MMS handshake time	MMS prof. exc. time	Total handshake time	RTT-report	RTT-setpoint	Retras mission
Plain security	**ETH**	0.000986	–	–	0.002477	0.103992	0.107455	0.001153	0.001411	0
	4G	0.04966	–	–	0.115076	0.308075	0.472811	0.12716	0.107341	3
Standard security	**ETH**	0.001159	0.047849	0.044036	0.002729	0.103911	0.155647	0.001157	0.001704	0
	4G	0.054625	0.132415	0.176210	0.076725	0.343444	0.607209	0.101212	0.107154	1.87
	3G	0.390826	1.229483	0.431360	0.54844	2.451566	4.620315	0.506906	0.498593	2.887
	2G	2.003555	5.64858	4.568160	3.694058	11.99704	23.34323	2.293466	2.293621	8.06

TLS Performance

The overhead brought by TLS on the different metrics can be easily taken from Table 1 considering the Ethernet network as base case. The results show that the inclusion of the TLS causes the increase of the time for each single communication phase, and introduces an extra time of 0.047849 s for the TLS handshake. We can conclude that the total time for the initial handshake and session phases is 0.107455 s without TLS and 0.155647 s including TLS security which means an overhead of 0.048192 s corresponding to a increment of 44.84% of the total time. Considering only the MMS Handshake and Profile Exchange Time indicators the impact of TLS is not so consistent. Also considering the RTT-Report and RTT-Setpoint indicators it is possible to note that the impact on the time is irrelevant (0.000004 s and 0.000293 s). Similar results may be inferred analyzing the trace from the 4G cellular test. Here it is important to consider the bias due to the unpredictability typical of the mobile networks for the presence of variable background traffic.

Cellular Technology Performance

The aim of this subsection is to compare the baseline technology (Ethernet) performance with the ones obtained considering different type of cellular access network. We focus on Standard Security scenarios, but an Ethernet vs 4G comparison considering Plain Security is also performed.

The magnitude of the total handshake time (see Fig. 4 and Table 1) in Ethernet test is of 100 ms, considering the 4G/LTE technology we have a value of 500/600 ms, but if we change the cellular technology we scale up of one order of magnitude with 3G (4600 ms) and of two orders with 2G (23300 ms). The values in Fig. 4 refer the mean value over the three DER sites for each of the run in the Short Tests. Considering 2G not all the DER values are available for all the run (means of the * symbol in the legend). The cellular results are deeply influenced by the TCP retransmissions occurring during the tests over the mobile network.

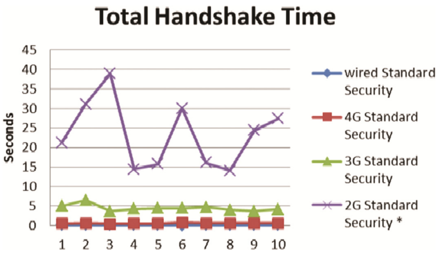

Fig. 4. Total handshake time

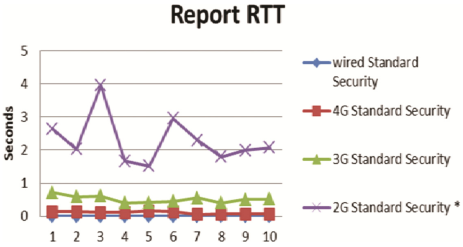

Fig. 5. Report RTT

If we focus on RTT values (see Fig. 5 and Table 1), we see that the gap between 4G and 3G is less evident (100 ms with 4G and 500 ms with 3G). The main step is between the Ethernet solution (1 ms) and 4G (100 ms) and between 3G (500 ms) and 2G (2290 ms). In Fig. 5 the means over the three DERs for each run is plotted. Also in this case for 2G test not all the DER values are available for all the run (marked with * symbol). From the test results it is clear that the 2G technology does not meet the availability and delay requirements of the VC application (neither those of the DER protection applications most probably sharing the same communication link). The 4G radio transmission seems to be provide acceptable performances. In case the 4G mobile coverage is not able to guarantee the service due to the DER site geographical position or the mobile network condition is degraded, the 3G technology can be a valid backup solution. Another important aspect to take into account for the right interpretation of the test results is the dependency of the evaluated indicators on the cellular network topology and condition: the size of the mobile cell, the relative position of the DER site within the mobile cell, the background traffic changing with the daytime and the weekday are all key parameters that influence the QoS results. We have to underline that the 4G/3G/2G network equipped for this test bed is a prototypal solution, to be improved also using the trial results here gathered to build a more satisfying implementation in order to meet theoretical RTT values of less than 20 ms.

5 Outcome and Future Work

This paper presented the implementation of a test bed to perform experiments on MMS communications according to IEC 61850 data models, among DSO substation and DER sites, over heterogeneous networks and end-to-end security through TLS encryption and authentication conforming to IEC 62351-3. Using the test traces obtained, the overhead of TLS and the impact on communication times of the cellular (in particular LTE) network are analyzed and discussed. These results represent a crucial step in order to allow the evolution of the security standards and to analyze the applicability of the different cellular technologies to critical smart grid applications. Because of the strongly experimental nature of the adopted M2M platform, the results obtained must be consolidated by running further tests under different network conditions. In the test bed setup used for these analyses, the features of TLS session resumption has been implemented within the MMS application but not quantitatively evaluated. Moreover, as a third test case with ICT fault or malicious attack has been implemented in the testbed, the application reconnection and the TLS session resumption after a network fault or attack could be investigated in the future.

Acknowledgement. This work has been supported by the European FP7 project SmartC2Net (under grant agreement no. 318023). Further information is available at www.smartc2net.eu.

References

1. SmartC2Net European Project, Deliverable D1.1: SmartC2Net Use Cases, Preliminary Architecture and Business Drivers, September 2014. http://www.smartc2net.eu
2. Moneta, D., Mora, P., Belotti, M., Carlini, C.: Integrating larger RES share in distribution networks: advanced voltage control and its application on real MV networks. In: Integration of Renewables into the Distribution Grid, CIRED 2012 Workshop, Lisbon, May 2012
3. International Standard IEC 61850-8-1 Ed. 2: Communication Networks and Systems in Substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, June 2011
4. ISO/IEC 8650-1 Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: Protocol specification, ISO (1996)
5. International Standard IEC 61850-7-420 Ed. 1: Communication networks and systems for power utility automation – Part 7-420: basic communication structure – distributed energy resources logical nodes, March 2009
6. International Standard IEC 62351-3 Ed. 1: Power systems management and associated information exchange - data and communication security – Part 3: communication network and system security – profiles including TCP/IP, International Standard, October 2014
7. Network Working Group TLS Version 1.2: The Transport Layer Security (TLS) Protocol, RFC 5246, August 2008
8. Latency and Bandwidth Analysis of LTE for a Smart Grid – Xu. http://kth.diva-portal.org/smash/get/diva2:565509/FULLTEXT01.pdf
9. libIEC61850 – open source library for IEC 61850. http://libiec61850.com/libiec61850/
10. OpenSSL: The Open Source Toolkit for SSL/TLS. https://www.openssl.org/
11. http://www.rse-web.it/laboratori/laboratorio/60
12. SmartC2Net European Project, Deliverable D6.3: Final results from laboratory tests, November 2015. http://www.smartc2net.eu