Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure

Juan Hoyos, Mark Dehus, Timthy X Brown
Interdisciplinary Telecommunications Program
University of Colorado Boulder
Boulder, Colorado, USA
{Juan.Hoyos, Mark.Dehus, Timxb}@colorado.edu

***Abstract*—Security issues for the power industry have become increasingly relevant during the past decade as the industry has relied more and more on communication protocols. The Generic Object Oriented Substation Events (GOOSE) protocol is defined in IEC 61850 for the purpose of distributing event data across entire substation networks. In this paper we demonstrate a practical attack by exploiting weaknesses in GOOSE. We also show that this attack can have devastating consequences on the reliability of the grid and is capable of creating a widespread interruption in power generation and distribution.**

Keywords; cybersecurity; GOOSE messages; IEC 61850; substation security; critical infrastructure.

I. INTRODUCTION

Security issues for the power industry have become increasingly relevant during the past decade. For more than 20 years almost all communication between devices inside and outside of power substations has been implemented using copper wires and legacy communication protocols [1]. There were many disadvantages to this approach, including long implementation schedules, the high cost of copper wiring, the few parameters available for monitoring, and the need for ongoing maintenance. IEEE 802.3 (Ethernet) based systems have overcome some of these problems by applying the same LAN solutions that have worked for more than 25 years in the Information Technology (IT) industry [2]. While the transition from analog to digital data acquisition allows the power industry to innovate with new communications technologies and protocols such as IEC 61850, it also poses new cybersecurity problems that can affect the stability and reliability of the power grid [3].

IEC 61850 provides a model and rules for organizing data in a manner that is consistent across all types of electronic Intelligent Electronic Devices (IEDs). Generic Object Oriented Substation Events (GOOSE) form part of the IEC 61850 protocol, embedding select logical and analog data such as circuit breakers status, circuit breaker control, interlocking, general alarms, and power transformer's temperature that are transmitted in Ethernet packets [4].

This paper demonstrates how to create computer malware that can capture, alter, and re-inject GOOSE messages into the network. By taking advantage of existing security holes in the GOOSE messaging protocol, we show how a malware could be used to significantly disrupt the power grid and highlights the need to apply security measures in this area.

The next section presents an overview of cyber-security for critical infrastructure, providing a brief history of cyber-security and the initiatives, which lead to the creation of current standards. Section III explains the main concepts of GOOSE and how to exploit weaknesses in its design to perpetrate an attack. Section IV demonstrates a practical attack against substation equipment. Section V and VI presents possible solutions to mitigate risks and conclusions.

II. CRITICAL INFRASTRUCTURE PROTECTION

A. History, Agencies, and Standards.

Critical Infrastructure (CI) protection is becoming an increasingly important topic internationally, and particularly after the events of September 11, 2001 in the United States. Federal laws mandate that any virtual or physical assets whose incapacity or destruction would have a debilitating impact on security, national economics, or national public health or safety must be considered CI [3]. The Department of Homeland Security (DHS) defines a total of 18 sectors for the U.S. and each sector is assigned to a specific government agency, which is responsible for identifying risks and promoting rules or standards to protect its assigned CI [5].

For energy-related CI, the Department of Energy (DoE) has been assigned to identify and promote best practices and methodologies for protection and continuity of energy services. The DoE has designated the North American Electric Reliability Corporation (NERC) as the organization responsible for assuring security of the power grid and elevating awareness and understanding of threats and vulnerabilities to utility assets, systems, and networks. In May of 2006 NERC released a set of Critical Infrastructure Protection (CIP) Cyber Security Standards, CIP-002 through CIP-009, applicable to users, owners and operators of the power grid. The CIP standards are designed to minimize the risk of possible cyber attacks using the communications infrastructure, as well as potential physical attacks either of which compromise the integrity of the grid [6].

There are other organizations such as the British Standards Institution (BSI), the National Institute of Standards and Technology (NIST), and the International Society of Automation (ISA) that are working on standards for cyber security for automation processes.

B. Cybersecurity for IEC 61850

In the early days of IEC 61850 there were no recommendations for security on the layer 2 multicast GOOSE and Sampled Measured Values (SMV) messages. The vulnerability was considered to be low because the messages were running in a confined network inside a substation protected by the physical

978-1-4673-4941-3/12/$31.00 ©2012 IEEE

network isolation. This is not true today when new applications are running GOOSE messages outside substations for wide-area transmission protection schemes and distribution automation schemes [7] [8]. Further, substations have become more connected to external networks and employ wireless networks with the potential to expose their IEC 61850 network to outside attackers.

In 2007 the same technical committee that develop the standard IEC 61850, IEC Technical Committee 57 (TC57) in the Working Group 15 (WG15), released the IEC 62351 standard to provide security to a number of TC57 protocols including IEC 61850 GOOSE messages.

The objectives of IEC 62351 are authentication of data transfers through digital signatures, prevention of eavesdropping, spoofing, and intrusion detection [9]. This provides security enhancements not only for Manufacturing Message Specifications (MMS) but also for GOOSE messages and SMV messages. Part 6 of the IEC 62351 standard covers data and communication security for IEC 61850 peer to peer profiles, part 3 defines the communication network and system message authentication profiles including TCP/IP, and part 4 specifies the mechanism of strong authentication to be utilized with MMS profile. These definitions provide manufacturers and integrators the tools necessary to implement security for IEC 61850 and the GOOSE stack [10]. Though IEC62351 addresses many security issues, problems remain.

C. The Problem of Encryption & Message Authentication versus Latency

Latency is one of the primary barriers to implementing security for peer-to-peer communications between IEDs. For instance, IEC 61850-5 specifies a 4ms maximum delay for class P1 type 1A GOOSE messages related to breaker trip functions [12]. As a result, encryption or other security measures, which increase the delay or latency, are avoided.

The IEC 62351 standard defines a mechanism that requires low computational power to authenticate the data adding a digital signature. The digital signature is created via mathematical techniques to validate the authenticity of a digital message using asymmetrical cryptography. This kind of scheme uses public and private keys to authenticate the message. The public key is shared with everyone to decrypt a hash of the message, while the private key is kept private by the publisher to sign the message. In the IEC 62351 standard part 6 states "for applications using GOOSE and IEC 61850-9-2 and requiring 4ms response times, multicast configurations and low CPU overhead, encryption is not recommended" [9]. Nevertheless the standard does not say anything about authentication and its limitation. Based on the ambiguity of authentication or encryption some manufacturers do not implement any security in their IEDs, arguing that any security mechanism will increase the processing time decreasing the speed of action against a fault.

At present it is difficult to reconcile the needs for security and low latency. One study conducted by Cambridge University and ABB in 2010 showed that processing (encoding and decoding) digital signatures required intense CPU consumption. Therefore, 32-bit Intel and ARM cores are generally incapable of computing and verifying a digital signature using the Rivest, Shamir and Adleman (RSA) algorithm with 1024-bit keys within 4ms [11]. The time for a digital signature to be generated at the sender and verified at the receiver is shown in Table I as well as other similar algorithms such as the Digital Signature Algorithm (DSA), the Elliptic Curve DSA (ECSDA), and the Boneh, Lynn, Shacham (BLS) scheme [13]. Although RSA is the fastest (8.3ms), this time is not enough to comply with the 4ms time constraint. In fact NIST in a report of 2011 qualified the RSA 1024-bits keys as acceptable through 2011, deprecated, from 2011 through 2013, and disallowed after 2013. After 2013 it is recommended to use 2048-bit keys, which will make the 4ms time restriction more difficult to meet [14].

TABLE I
TIME TO GENERATE AND VERIFY A DIGITAL SIGNATURE ON A 1.0 GHZ PENTIUM III PROCESSOR FOR DIFFERENT SCHEMES [13]

Algorithm	Generation Time (mSec)	Verification Time (mSec)	Bandwidth (bits)
RSA	7.9	0.4	1024
DSA	4.1	4.9	320
ECDSA F_{2160}	5.7	7.2	320
ECDSA F_p	4.0	5.2	320
BLS F_{397}	3.5	23.0	170

The central processor unit (CPU) embedded in the IEDs has some restriction due to the power dissipation. The IEDs are fan-less; installed commonly in closed cases to avoid environmental issues like dust, water, or insects. Thus, many embedded processors are slower than the 1.0 GHz processor used in this table and times will be even longer. New technologies like multiple cores may enable faster times within the same heat dissipation budget. However, there are many IEDs already installed in the market with slower CPUs.

Currently neither the IEC 62351 recommendation nor proprietary manufacturer solutions have been implemented extensively to improve the security of GOOSE messages. In November 2011 Siemens published a patent to implement a new method of group key generation and management for the GOOSE model that could help to address the need for low latency security [15]. Meanwhile there is little clarity on how to implement security for fast GOOSE messages without degrading the actual performance of the IEDs.

III. EXPLOITING THE GOOSE PROTOCOL

A. Normal GOOSE Function

The main objective of GOOSE messaging is to provide a fast and reliable mechanism that allows the exchange of data between two or more IEDs over IEEE 802.3 networks. To exchange these datagrams, IEC 61850-8-1 describes a type of communication based on a publish/subscribe model, where one IED (the publisher) creates a message that is delivered to a group of destination IEDs (the subscribers) simultaneously in a single transmission from the source [4].

GOOSE messages are periodically sent through the network. When there is no change in data set values, the retransmission time between messages is T_0 (see Fig. 1). If an event occurs a message is generated immediately. After the first event message the publisher retransmits (T_1, T_2, …, T_N) with a variable time separation between messages that is not defined by the standard, but is typically implemented following an exponential back-off, until it reaches the stable retransmission

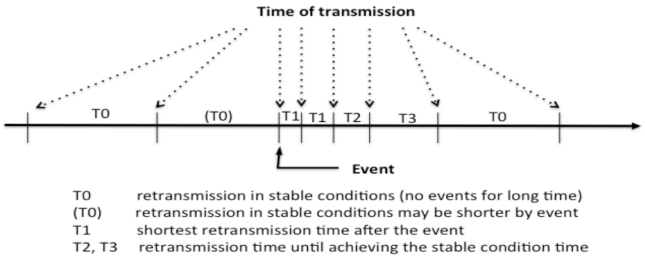

Fig. 1. GOOSE transmission [4]

time T_0. If T_0 is exceeded, the subscriber could declare a problem in the communication link or in the GOOSE message [4].

The GOOSE datagram has twelve fields that define the Protocol Data Unit (PDU), the first two fields, **preamble** and **start** of frame, are equal to the first two fields of an Ethernet frame. The **destination** corresponds to an Ethernet MAC multicast address. IEC 61850 has been assigned Ethernet addresses that start with the three first octets (01-0C-CD). The fourth octet could be 01 for GOOSE, 02 for GSSE, or 04 for multicast SMV. The last two octets of the six are used as individual addresses for each GOOSE message. The **source address** is a unicast MAC address. The **VLAN priority tagging** is IEEE 802.1Q. The **Ether-type** of a GOOSE message is 88-B8. The **Application ID** is 00. The **length** indicates the total number of bytes in the frame less eight bytes. The **Reserved1** and **Reserved2** fields are reserved for future standardized applications and are set to 0 by default. The last two fields are the **Application PDU (APDU) length** and finally the **frame checksum sequence** [4].

The APDU has ten fields described here. **DatSet** is a string that describes the name of the Data Set. **GoID** is the IED sender identifier. **T** is the "time-stamp" at which the attribute StNum was incremented. **StNum** is the "State Number", a counter that increments each time a GOOSE message has been sent with any change in the values of the Data Set. The **SqNum** is the "Sequence Number", containing an incremental counter for each time a GOOSE message has been sent. The **Test** field indicates if the message is a test or not. **TimeAllowedToLive** is the time that the receiver has to wait for the next message. **ConfRev** is the "Configuration Revision", a count of the number of times that the configuration of the Data Set has been changed. **NumDatSetEntries i**s the "Number of Data Set Entries", the number of elements that comprise this specific data set [4].

B. Attack Vectors and Techniques

An attack is defined by the motivation, vectors, and the techniques. In this paper, we assumed a motivated attacker and focus on the attack vectors and techniques.

The attack vector is a path or means by which an attacker gains access to a computer or network in order to achieve their ultimate goal. Attack vectors enable exploitation of the system vulnerabilities, including human elements. Access to the network could be obtained via installation of malware on the computers of maintenance operators, engineers, or manufacturer support teams who access a GOOSE network and are unknowingly carrying the malware. A similar attack vector was used to allow the Stuxnet worm to gain access for an attack on Siemens industrial software and equipment in 2010 [16].

An attack vector can come from malicious persons among cleaning crews or substation personnel that have access to the IEC 61850 network. Another attack vector is through manufacturing facilities of producers of IEC 61850 IED equipment or other network equipment. Such equipment can be infected with malware at the time of manufacture and installed directly in a substation, bypassing physical protection and providing the malware with a host. The attacks that we describe can be hosted on even simple devices.

There are several layer 2 attack techniques that could be applied to GOOSE message since the underlying IEC 61850 network is Ethernet. Attacks on Ethernet include: ARP attacks, MAC flooding attacks, spanning-tree attacks, multicast brute force attacks, VLAN trunking protocol attacks, private VLAN attacks, identity theft, VLAN hopping attacks, MAC spoofing and double-encapsulated 802.1Q/Nested VLAN attacks. An attack could be created using a variety of techniques described above, and the structure of protocols in the OSI model are such that the upper layers in the model could be unaware that layer 2 has been compromised [17].

C. Attack Consequences

There are several consequences if a layer 2 attack is executed in a substation. The main purpose of the GOOSE message is to carry vital information (alarms, status, and control) between devices. Any alteration of these values could create an automation breakdown, causing a circuit breaker to miss an operation, bypassing interlocks, or causing physical damages in the field devices like power transformers or circuit breakers. If the attack compromises a bus bar or differential protection, more than one distribution or transmission circuit could be affected. As a result one part of the city or region would suffer an outage. If the same attack involved transmission or generation circuits, the outage could trigger cascading failures and become sufficiently large so as to affect complete cities or states.

As a specific example, the Palo Verde Nuclear Generating Station (PVNGS) and California ISO use GOOSE messaging between their substations to create a Remedial Action Scheme (RAS) on the Salt River Project. The GOOSE messages are implemented in a "flat" Ethernet Ring and carry analog and digital values to control the load at both sides. Measured changes in generation levels on one side of the system must affect load balance on the other side of the system over 150 miles away in less than one second. A GOOSE attack that appears to changes the values of generation levels could produce voltage dips, frequency excursions, and cascading problems throughout the Western Electricity Coordinating Council (WECC) region [8].

IV. Building a Practical Cyber Attack

A. Technical Details

The following attack was implemented as an ethical demonstration of security vulnerability in the Digital Energy Laboratory at the University of Colorado Boulder, with details of the equipment and scripts intentionally omitted. A similar attack could move from the lab to the field in a matter of days.

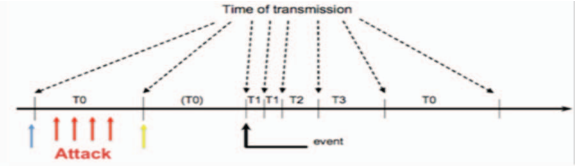

Fig. 2. GOOSE attack schematic

Our attack uses a GOOSE exploit via spoofing where an intruder publishes false layer 2 packets and devices on the receiving side mistakenly believe they are receiving valid (true) packets sent by a trusted or secured entity. This attack is possible due to the unencrypted & unauthenticated nature of GOOSE messages, owing to the latency issues on IED devices as previously detailed.

A practical GOOSE message spoof attack can be divided into four steps. First, monitor packets on the physical ports looking for GOOSE messages based on Ether-type identification. Second, decode the GOOSE message using Abstract Syntax Notation One (ASN1) and Basic Encoding Rules (BER) [18]. Third, change the values inside each data set, keeping the sequence for the different counters and timers. Fourth, encode the packet using BER and send the packet through a physical port cloning the source MAC address. The schematic in Fig. 2 shows how the attacker has an opportunity between each valid message to insert the spoofed messages with incorrect data.

There are several programs that can be used to do this: Scapy, Yersinia, Macof, TCPDump, Cain & Abel, EtterCap, Wireshark, etc. This attack was created using Scapy in conjunction with Python scripts. Scapy is also a Python program that enables the user to sniff, dissect, forge and send network packets. These capabilities allow the construction of tools that can probe, scan, or attack Ethernet networks.

To prove the vulnerability of the GOOSE networks our attack script uses the network configuration shown in Fig. 3, which represents a typical substation automation architecture. In addition new scenarios were created, such as GOOSE messaging between substations using Layer 2 tunneling and wireless communications inside the substation. The lightning bolts in the Fig. 3 represent the attack points. The attack was successful in all scenarios and we describe one in detail below.

The hardware used for the test were two (2) Cisco 3600 Routers, one RuggedCom 2100 switch, one RuggedCom RS900, one Linksys wireless router, and four IEDs. The script ran on a MacBook Air 1.5Ghz Intel core i5 within a virtual machine running Xubuntu OS.

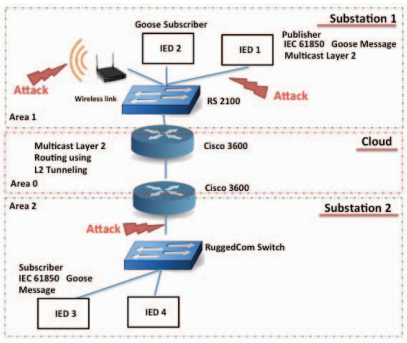

Fig. 3. Network Diagram

B. Building the Script

The first step to carry out the attack is to identify GOOSE messages in the network. After using Scapy to monitor all physical ports and capture the raw packets, the code parses the Ethernet frames looking for the specific GOOSE Ether-type, which in this case is 0x88B8. Second, it is necessary to decode the GOOSE message using the definition of ASN1 described in the IEC 61850-8-1. After decoding, the script looks for three specific fields: stNum, sqNum, and the Boolean values inside the data sets. For any Boolean value inside the data-set, if the value is true the code overwrites a false and vice versa.

The last part of the code generates the spoofed messages and sends them through the network with the same source and destination MAC address as the valid user. To show the attack can be successful, we implemented the above steps on the laptop described above.

C. The Results of the Attack

Figure 4 shows a Wireshark capture, where the topmost and the bottommost arrows are the true messages. The four middle arrows, events 194 to 197, are the spoofed messages. Looking at the time stamp of the packets 193 and 195, the time to generate spoofed GOOSE messages is less than 1ms. This means that in a default GOOSE configuration, where the messages are sent at 1 second intervals during steady state, the attack could inject hundreds of false GOOSE messages before the next valid datagram reaches the IED.

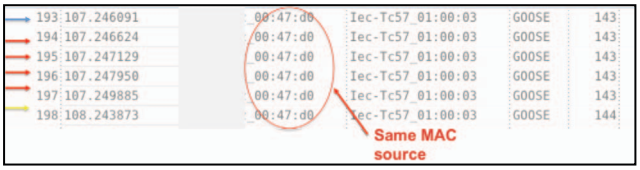

Fig. 4. Wireshark capture showing spoofed GOOSE messages

The process of modifying data is illustrated in Fig. 5, which shows the variable values in three successive GOOSE messages measured by the laptop at the RuggedCom 2100 in Fig. 3. The leftmost message is a valid message. The attacker created the next message in the middle. It shows the change of stNum, which resets the SqNum in the cloned packet. The rightmost message is the next valid message. This keeps on the old number sequence, which means that it is out of sequence. We note that the equipment did not generate any error or warning that the messages are out of sequence.

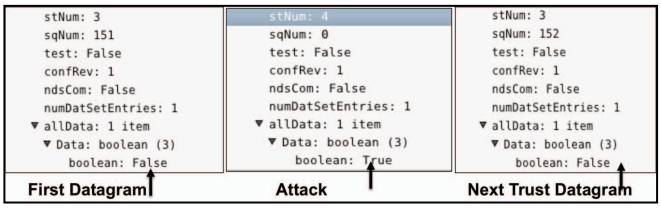

Fig. 5. GOOSE exploit

The attacker does not directly know the high-level meaning of this GOOSE message (e.g. that this is a command from a circuit-breaker controller to a circuit breaker). However, it can decode the message to find and change the Data values. In Fig.

5, the attacker changes the Boolean data value from False to True. To verify this has an effect, Fig. 6 shows the Sequence Event Recorder (SER) on the IED. This SER monitors the physical outputs and generates a time stamp of output events.

Event 4 (number on the left) shows the times when the valid message instructed the IED to deassert output 101. After 5ms a spoofed message is processed at the IED asserting the output and generating event 3. Another 995ms later the next true message arrives, generating the event 2, which again deasserts the output. In this case, the effect of this action is to cause the IED to trip the relay. The relay in a real substation could control a circuit breaker or switch.

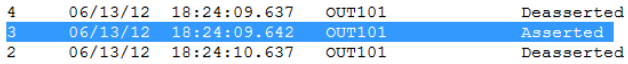

Fig. 6. IED output status

V. How to Mitigate This Kind of Attack

Although some attack vectors could be reduced using physical security, there are others that are more difficult to control because they use trusted personnel or equipment.

Some classical IT techniques to prevent Ethernet layer 2 attacks could be applied to protect GOOSE messages. These practices include but are not limited to: set a dedicated VLAN ID for all trunk ports, disable unused ports and put them in an unused VLAN, use a VLAN other than the default (VLAN 1), set all ports to non-trunking, create an access or prefix list based on user/device credentials, avoid the use of shared Ethernet such as WLANs or hubs [19]. All of these techniques are well documented and known by IT staff.

At this level using the measures indicated the network is somewhat protected against intrusion originating from outside of the organization. For trusted employees or compromised equipment inside the facility, which have valid credentials, most of the traditional IT techniques would be ineffective. Therefore additional security measures must be implemented.

To prevent insider attacks it is necessary that end devices have security algorithms implemented to encrypt packets or add a digital signature so that they cannot be monitored by the attacker and authenticated so that spoofed packets cannot be sent. As noted in Section II-C, legacy and low-capability IEDs cannot support these cryptographic algorithms.

Solutions like adding an external security module to network interfaces in each IED adds expense and additional failure modes. These techniques could be added just to the switches and some key equipment in the Ethernet to provide some limited protection. An alternative approach could use switches and routers that understand the IEC 61850 protocol and inspect GOOSE message content. In this approach, the network could discard or generate alarms when it detects logically inconsistent messages (such as packets with the same MAC address coming from different ports on a switch or messages not consistent with the IEC 61850 configuration).

VI. Further Work

The lack of clarity in the standards about how to implement the security for IEC 61850 layer 2 messages with the current technology opens the door to new research. Additional research could focus on security measures and standards that could be backwards compatible allowing for thousands of IEDs to be able to run layer 2 multicast protocols securely.

VII. Conclusion

We demonstrated that a simple attack enables malware to control IEC 61850-enabled control equipment. This control has the potential to cause outages that range from a single feeder on up. While there is no clear definition about how to implement security for GOOSE messages, utilities and power companies must implement not only physical but also cyber measures to prevent this kind of attack. We describe several techniques for improving security not only for physical but also networking self-configuration measures. Meanwhile, it is of vital importance that the configuration of the network switch and routers be permitted just for trusted traffic and users inside the substation network.

Acknowledgement

This work was supported by Department of Energy grant DE-OE00436 and by Empresas Públicas de Medellín E.S.P. RES 543-2011.

Bibliography

[1] R. E. Mackiewicz, "Overview of 61850 benefits", *Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES*. 21-24 May 2006, pp. 376 – 383, doi: 10.1109/TDC.2006.1668522

[2] G. Scheer and D. Dolezilek, "Comparing the reliability of Ethernet network topologies in substation control and monitoring networks". Technical Applications Document. SEL, Pullman, WA, April 2000, [Online]. Available:
http://www2.selinc.com/techpprs/6103.pdfhttp://www2.selinc.com/techpprs/6103.pdf

[3] Department of Homeland Security. "Information analysis and infrastructure protection". *Critical Infrastructure Information Act of 2002,* [Online]. Available:
http://www.dhs.gov/xlibrary/assets/CII_Act.pdf

[4] IEC, *Communication networks and systems in substation -- Specific communication service mapping.* IEC 61850.8, 2008.

[5] Department of Homeland Security, National infrastructure protection plan, partnering to enhance protection and resilience. May 2 2009, [Online]. Available: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[6] NERC, *NERC Implementation plan for cyber security standards CIP-002-1 through CIP-009-1*, 2006. Available:
http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-0

[7] M. Goraj, L. Lipes, and J. McGhee, "IEC 61850 over Wimax for fast isolation and restoration of faults in distribution networks", *PacWorld Conference,* 2011. Available:
http://es.scribd.com/doc/78041627/74994185-Iec-61850-Goose-Over-Wimax-Pac-World-2011

[8] M. Adamiak and G. Brunello. "Implementation and operational experience of a wide area special protection scheme on the SRP system", *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources,* 2006, pp. 145-158, doi:10.1109/PSAMP.2006.285384

[9] IEC, *Power systems management and associated information exchange, data and communication security*. IEC standard 62351, 2007.

[10] H. Falk, "Securing IEC 61850", *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century,* July 2008, pp. 1-3, 20-24, doi: 10.1109/PES.2008.4596335F

[11] Alvarez, K. Hansen, and K. McGrath. "The Protection of Substation Communications". *Proc. of S4 2010: SCADA Security Scientific*

Symposium, January 2010, Miami, USA Available: http://www.cl.cam.ac.uk/~sf392/publications/S4-2010.pdf

[12] IEC, *Communication networks and systems in substation, Specific communication service mapping*. IEC standard 61850.5. 2008.

[13] Brian J. Matt, "The cost of protecion measures in tactical networks," *Proc. of the 24th Army Science Conference* 29 November - 2 December 2005, Orlando, Florida http://www.dtic.mil/dtic/tr/fulltext/u2/a432010.pdf

[14] Elaine Barker and Allen Roginsky, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST Special Publication 800-131A http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[15] S. Fries and M. Seewald. "Method of group key generation and management for generic object oriented substation event model". International Patent WO2011/141040A1, November 17, 2011.

[16] R. McMillan, "Siemens: Stuxnet worm hit industrial systems". *Computerworld*, September 14 2010 [Online]. Available: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems

[17] L. Senecal, "Understanding, preventing, and defending against layer 2 attacks" *Cisco Expo 2009*. [Online]. Available: http://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf

[18] ITU, *Information technolog ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. ITU Standard X.609, 2002 [Online]. Available: http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf

[19] Yunsuf. *CCIE profesional development series network security technologies and solutions*, Cisco press, March 20 2008, pp. 221, ISBN 1-58705-246-6.