Wide Area Protection & Control using High-Speed and Secured Routable GOOSE Mechanism

Mital Kanabar, Anca Cioraca, Anthony Johnson

***Abstract*—WAPC using Routable-GOOSE (R-GOOSE) is an emerging solution to improve power system protection, control, and monitoring. The R-GOOSE mechanism is a routable extension (IP layer-3) of already proven Ethernet layer-2 high-speed GOOSE within a substation. Comparison of Synchrophasor and R-GOOSE is examined considering protocol mechanisms, WAPC applications, network and bandwidth, performance/delay requirements perspective. A practical use case of R-GOOSE applying to Centralized Remedial Action Scheme (CRAS) is presented. Finally, advancements in cyber security technology to enable WAPC applications are discussed in details.**

***Index Terms*—Generic Object Oriented System Event (GOOSE), System Integrity Protection Scheme (SIPS), Wide Area Protection and Control (WAPC).**

I. Introduction

WIDE Area Protection and Control (WAPC) are deployed to protect the integrity of the power grid or strategic portions of the grid. Unlike conventional (mainly local) protection, WAPC are installed to achieve System Integrity Protection Schemes (SIPS), special protection schemes, Remedial Action Schemes (RAS) or backup protection to conventional protection systems, such as wide area differential protection using synchrophasors [1]-[3]. WAPC can be implemented among substations (distributed) or between substations and control center (centralized). The backbone of the WAPC scheme is networking infrastructure and engine is a protocol to exchange information over Wide Area Network (WAN). The major communication infrastructure considerations for WAPC system are: 1) High-speed message delivery (short delays over WAN); 2) network bandwidth requirement (i.e. optimum information/dataset and data rate); 3) cyber security; 4) Availability/Redundancy; 5) compliance to international standardized protocols. IEC Technical Report (TR) 61850-90-5:2012 provides communication protocol for synchrophasors (Routable-Sampled Values or R-SV) and event-driven GOOSE[1] (Routable-GOOSE or R-GOOSE) with embedded cyber-security into protocol over WAN [4].

This paper presents implementation of high-speed and secure R-GOOSE for WAPC applications, and also discusses a practical use case of Centralized Remedial Action Scheme (CRAS) project by Southern California Edison (SCE) at approximately 100 (primarily 500kV and 230kV) substations.

M. Kanabar, and A. Cioraca are with GE Grid Solutions, Markham, Ontario, Canada (e-mail: mital.kanabar@ge.com).

A. Johnson is with Southern California Edison (SCE), CA, USA.

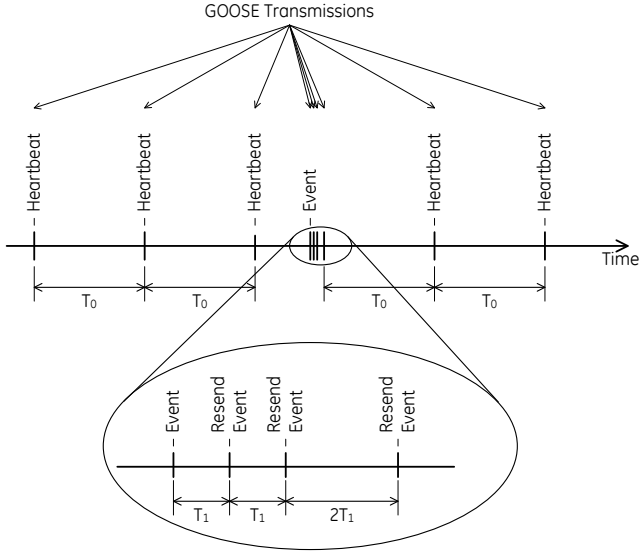
II. How to Implement GOOSE with Routing, High-Speed, and Security?

GOOSE is an industry recognized mechanism for time-critical peer-to-peer communication among Intelligent Electronic Devices (IEDs) [5]-[8].

A. Current GOOSE Operation

IEC 61850-8-1 standard specifies the GOOSE. GOOSE characteristics are: 1) Event driven with re-transmission; 2) high-priority and Virtual LAN support (IEEE 802.1Q); 3) peer-to-peer based publisher/subscriber communication (unlike client/server or master/slave); 4) multicasting over LAN (i.e. simultaneously publishing to multiple subscribers); 5) dataset items include both status information (digitals) or measurements (analog).

To achieve a highly dependable level of GOOSE message delivery, the IEC 61850-8-1 specifies a retransmission scheme for GOOSE messages, as shown in Fig. 1. When none of the dataset items in a transmitting GOOSE are changing, the GOOSE message is sent periodically (heartbeat) to allow subscribers to monitor the connection. When any dataset item state changes, the GOOSE message is re-transmitted immediately multiple times with the new values, shown as Event messages. A short time after the initial event message is sent, it is resent several times.



T_0 - TxGOOSE UPDATE TIME setting value

T_1 - TxGOOSE1 RETRANS TIME setting value

Fig. 1 GOOSE re-transmission mechanism.

B. Routing GOOSE over WAN

Until recently, GOOSE was specified for local applications

over LAN only, i.e. within substation, power plant or industrial sites. A technical report IEC TR 61850-90-5:2012 extends the application of GOOSE from LAN to WAN, either using tunneling or allowing GOOSE to multicast over IP networks using IGMPv3 protocol. These R-GOOSE messages are routed over layer-3 routers with UDP/IP headers. Security mechanisms for WAN are also called out in IEC TR 61850-90-5:2012 and enable several applications of high-speed and secured R-GOOSE for WAPC.

1) Multicasting over IP networks

Fig. 2 illustrates the communication stack from IEC TR 61850-90-5. The technical report specifies IGMP version 3 (RFC 3376) [9] for multicasting of R-GOOSE. IGMPv3 extended the capabilities of the protocol by allowing source filtering, which means that the routers are informed of the sources of the traffic.

Three different Application Profiles (A-Profiles) are specified in IEC/TR 61850-90-5. Each of these A-Profiles makes use of three independent Transport Profiles (T-Profiles). The correlation between the A-Profiles and T-Profiles is shown in Fig. 2. Various T-Profiles have common elements for the Network and Layer 2 layers. However, there are some differences within the Transport layer.

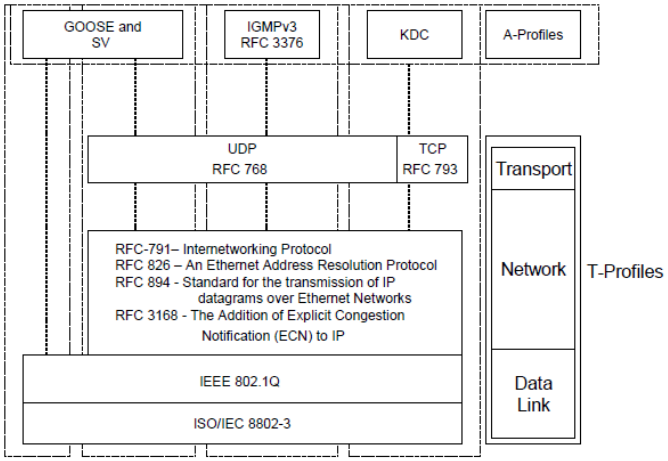


Fig. 2 Communication stack from IEC TR 61850-90-5 [4].

Attribute name	Attribute type	Value/value range/explanation
PRIORITY	Unsigned8	IEEE 802.Q priority
VID	Unsigned16	VLAN ID
APPID	Unsigned16	As defined in Annex C in IEC 61850-8-1
TransportInUse	Unsigned8	Enumerated value: IPv4, IPv6, and DNS assigned
IPClassOfTraffic	Unsigned8	TypeOfService value or Class of Traffic field.
IPv6FlowLabel	Unsigned32	Only with IPv6
IPAddressLength	Unsigned8	4 for IPv4, the value shall be four (4); 16 for IPv6
IPAddress	OCTET-STRING	This attribute shall be 64 octets in size.

Fig. 3 UDPCOMADDR structure [4].

2) R-GOOSE Control Blocks

IEC TR 61850-90-5 defines new Control Blocks to handle the Routable 90-5 semantics. "RG" control blocks are used to control routable GOOSE state information. Destination address attribute type is changed to UDPCOMADDR, which is shown in Fig. 3. This configuration allows UDP/IP header over the GOOSE.

3) Priority over IP

IP Class of Traffic (CoT), also known as TypesOfService (ToS), as shown in Fig. 3, is used to provide high speed quality of service. The encapsulated application messages are published via UDP/IP multicast services, which use the Differentiated Service Code Protocol (DSCP) to provide IP priority tagging for high-speed processing at the router.

C. Securing R-GOOSE over WAN

IEC TR 61850-90-5 security mechanism for R-GOOSE has the following options: 1) None; 2) Signature (i.e. Authentication); 3) Signature and Encryption. IEC TR 61850-90-5 security specifies the use of a signature using symmetric keys being applied to create a secure Hashed Message Authentication Code (HMAC). The application messages are carried over IEC 61850-90-5 session layer, which provides security and management via the 90-5 specific Group Domain of Interpretation (GDOI) protocol. GDOI support for 61850 protocols is described in the updated revision of IEC 62351-9 [10], and the key exchanges use Group Domain of Interpretation (RFC 6407 – GDOI) [11], [12].

III. Comparison of Synchrophasor and R-GOOSE for Wide Area Applications

Two technologies, synchrophasor and R-GOOSE, are available to achieve WAPC, and are compared in this section.

A. Synchrophasor vs R-GOOSE mechanisms

Wide Area Measurement System using synchrophasor standards (i.e. IEEE C37.118.1/2: 2012) [13] are already under deployment at large scale over the power grid [14]. Table 1 provides overall comparison of R-GOOSE and synchrophasor.

Table 1 Synchrophasor versus R-GOOSE

Parameters	Synchrophasors	R-GOOSE
Publications	IEEE C37.118.1/.2 :2012	IEC TR 61850-90-5 :2012
Communication	Client/Server (IP Unicast)	Publisher/Subscriber (IP Multicast)
Data transmission	specified rate, 1Hz to 120 Hz	Event-driven (1-2 Hz for no event; retransmission for events)
Data items	Synchrophasors, Analog, Digital	Analog and Digital (status)
Security	No	Key Distribution Center (KDC)
Priority	Regular (due to high data rate)	Higher (Event driven)
Networks	Regular IP/Layer-3 Router	IP/Layer-3 Router with IGMPv3 (firewall to support as well)
Configuration	CFG frames (CFG-1, 2)	ICD, CID files; GET services

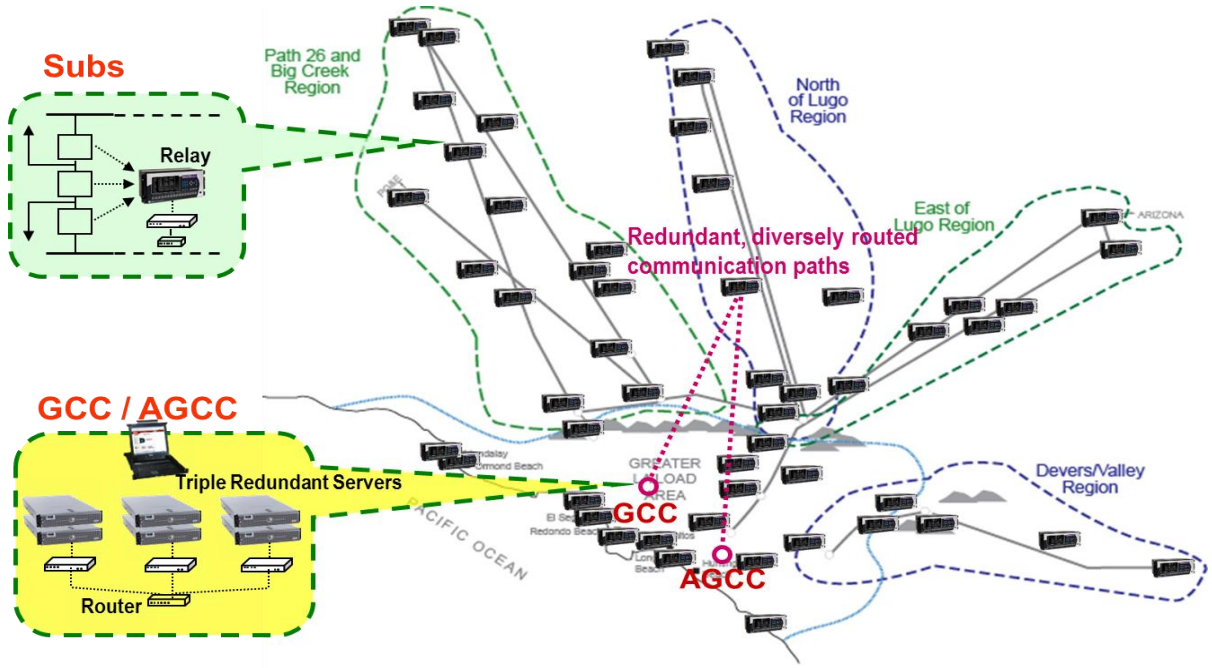


Fig. 4 Overall architecture of a typical Centralized- Remedial Action Scheme (C-RAS).

Major differences between synchrophasor and R-GOOSE are:

1) R-GOOSE are event driven, hence, the messages are transmitted at higher rate only in case of an event; whereas synchrophasors are transmitted at regular interval configured by the user.
2) R-GOOSE doesn't include synchrophasors (phasors calculated with reference to Global Time Reference-GPS clock) data values. IEC TR 61850-90-5 specifies separate mechanism called Routable-Sampled Values (R-SV) for the synchrophasor communication.
3) The same R-GOOSE can be multicast to multiple locations, however, network infrastructure must support IGMPv3, and firewalls cannot block the IGMPv3 traffic.

B. Applications Perspective

There are several WAPC/SIPS applications that do not rely on synchrophasor values. R-GOOSE suitable applications are as follows:

1) Load/Generation rejection based SIPS/RAS
2) System Separation/Islanding (unstable loading, angle, voltage, frequency conditions) based SIPS/RAS
3) UFLS (Under-Frequency Load Shedding)
4) UVLS (Under-Voltage Load Shedding)
5) Real-time system state determination application

C. Network and Bandwidth Requirements

Table 2 provides simple calculations of both mechanisms assuming equal frame size. Synchrophasors are transmitted 30 frames/second (configured); whereas R-GOOSE, which consider 1 event per second, are transmitted at approximately 5 frames per second.

Table 2 Synchrophasor and R-GOOSE comparison on communication

Parameters	Synchrophasors	R-GOOSE
Frame size	100 Byte	100 Byte
Data rate	30 frames/sec	5 frames/sec (worst case-1 event per second per device)
Number of devices transmitting	100 devices	100 devices
Byte Per Second over network	100*30*100=300000 Bytes/sec	100*5*100=50000 Bytes/sec (worst case)
Bandwidth requirements	300000*8=2.4Mbps	50000*8=0.4Mbps (worst case)
Number of locations/devices data received	1	Many (IP multicast)
Storage requirements per Year	300000 *3600*8760= 9.4 Tera Bytes	50000*3600*8760= 1.6 Tera Bytes (worst case)
Typical performance requirements	100 milliseconds to few seconds	<10 ms

D. Performance Requirements Perspective

A key parameter to choosing between synchrophasors and R-GOOSE is the relative priority of communication and latency. Synchrophasor system latencies are in the range of 100 ms to few seconds [15], due to higher data volume, whereas the typical delays of R-GOOSE are <20 ms (or even less if the network is designed properly).

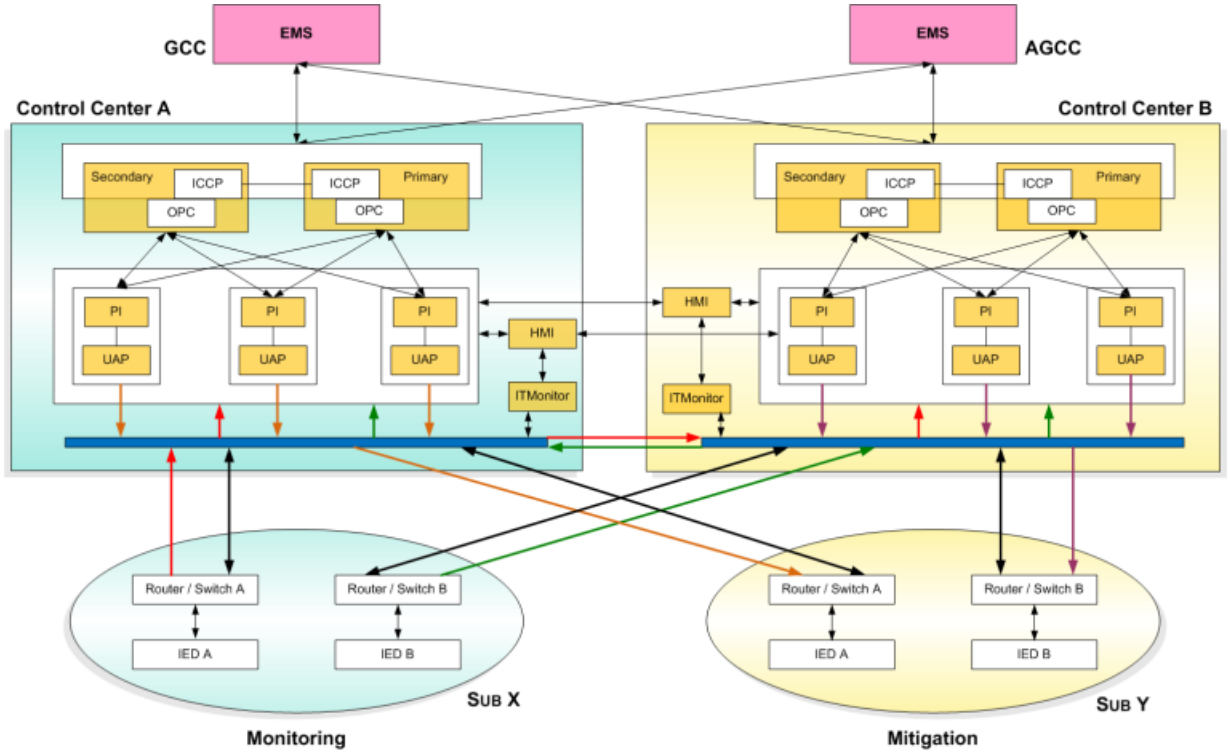


Fig. 5 CRAS with redundancy.

IV. USE CASE: R-GOOSE FOR CENTRALIZED-RAS

This section describes an R-GOOSE use case for Centralized Remedial Action Scheme (CRAS) project which replaces existing individual RASs, as shown in Fig. 4. CRAS implements special protection schemes that enable an automatic protection system to maintain system reliability by detecting abnormal or predetermined system conditions and taking corrective actions other than (or in addition to) the isolation of faulted components [16]-[18].

The main functional components of CRAS include (1) field devices (monitoring and mitigation devices); 2) communications networks (IGMPv3 enabled Gigabit Ethernet/IP links); 3) Central Controller Systems (CCS). There will be approximately 100 substations, most of which are 500kV and 230kV substations, to be equipped with monitoring relays or mitigation relays [19].

A. *Redundancy Considerations*

The system is fully redundant with duplicated A and B subsystems operating in parallel, as shown in Fig. 5. Each A or B subsystem will have its own CCS, monitoring relays, mitigation relays, and communication network infrastructure (complete independent system). The central controller for each A or B subsystem is designed with triple redundancy (2-out-of-3 voting) and installed in secure and geographically separated locations: Grid Control Center (GCC) and Alternate Grid Control Center (AGCC). Each substation will have two sets of relays, one for C-RAS A, and the other for C-RAS B. Between GCC and AGCC, there will be two redundant and diversely routed Gigabit Ethernet links to exchange System A and System B information coming from the substations.

B. *Performance Requirements*

Of the entire system performance budget, three cycles (e.g. approximately 50 ms) are allocated to communication and controller/logic latency. Of the 50 ms, 38 ms are designated for communication latency and 4 ms for controller reaction time, shown in Fig. 6 [20]. The 50 ms allows for an operational variance of 8 ms.

1 cycle = 16.7 milliseconds

	Time	Operational Events	
Step 1	@ 0 Cycle	3 Phase Fault on the Bus	Event Detection Fault Clearing:
Step 2	@ 1 Cycle	Relay Processing time for trip signal to CBs	
Step 3	@ 5 Cycles	Open CBs for line/transformer out	
Step 4	@ 7 Cycles	RAS Logic Processing for trip signal to CBs to trip generators	RAS Processing:
Step 5A	@ 10 Cycles	Open CBs associated with 12 generators (I Batch Mitigation)	Mitigation Generation Tripping / Load Shedding:
Step 5B	@ 12 Cycles	Open CBs associated with 4 generators (II Batch Mitigation)	
Step 5C	@ 16 Cycles	Open CBs associated with 2 generators (III Batch Mitigation)	

Fig. 6 Performance requirements for load/generation tripping scheme [20].

C. *R-GOOSE Datasets*

Relays at the substations are either monitoring or mitigating relays. Monitoring relays report loading of critical lines to the central controllers every few seconds. They also report trips of these lines – normally due to relay action – within milliseconds so that the controller can implement a strategy to mitigate the resulting overload on the remaining lines and preserve system stability. Mitigating relays at substations or generating locations receive control commands from the

central controllers to shed load or generation. The relays in a substation have their communications isolated to either System A and System B. A particular substation may have both monitoring and mitigating relays.

V. Implementation of Secured R-GOOSE for WAPC

A. Cyber Security Architecture

The key management is based upon Group Domain of Interpretation (RFC 6407 – GDOI) [11]. GDOI provides the capability of a Key Distribution Centre (KDC) to provide symmetric keys securely via either clients requesting the keys or the KDC pushing keys to the appropriate subscribers. GDOI originally allowed keys to be associated with IP addresses only. This proved insufficient for the security model/requirements for IEC TR 61850-90-5. Therefore, the GDOI protocol was extended by the report to provide key management based upon destination addressing, service, and DataSet definitions. This allows keys to be assigned and managed based upon the delivery service e.g. GOOSE or SV, even if the destination address and DataSet contents are the same, as illustrated in Fig. 7.

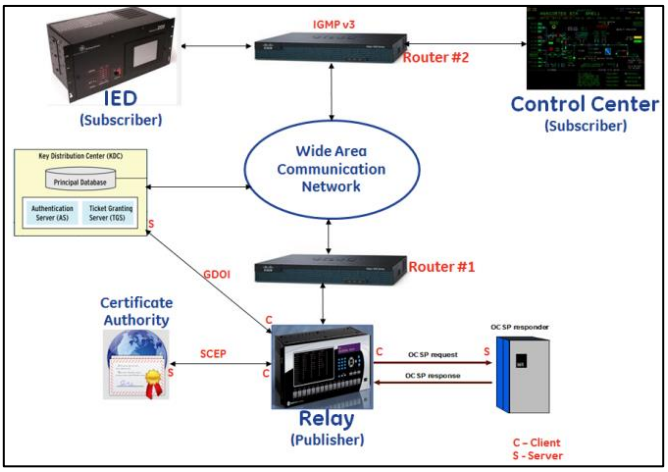


Fig. 7 R-GOOSE Security Architecture (simplified version).

B. Establishing Secure Communication for WAPC

Fig. 8 illustrates the simplified sequence of events to establish secured communication among R-GOOSE publisher and subscribers.

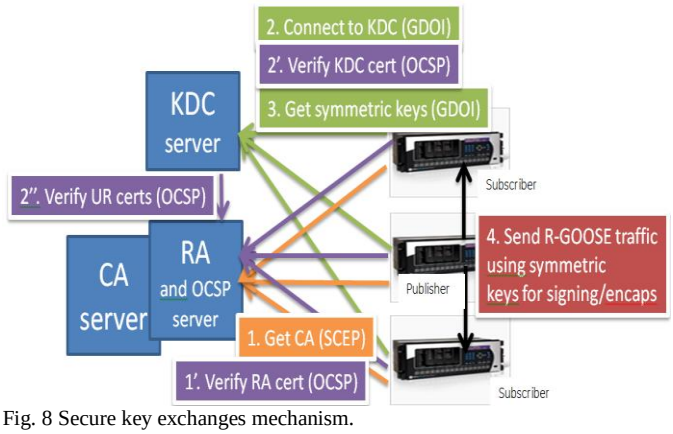


Fig. 8 Secure key exchanges mechanism.

There are two major exchanges involved: 1) Certification which is used to authenticate all devices exchanging keys; 2) Security Association (SA), followed by the distribution of symmetric keys used by the publisher/subscriber for signature and encryption.

The step-1 for providing R-GOOSE security support on device is dedicated to obtaining a certificate. The device uses the Simple Certificate Enrollment Protocol (SCEP) protocol for communication with the Registration and/or Certification Authority (RA/CA) and downloading the X.509 certificate.

Once the certificate is obtained, Publisher/subscriber initiates the second step (2), which is connection establishment with KDC server using GDOI protocol, as described in IEC 62351-9. Device sends its own certificate to KDC and requesting KDC's certificate.

As part of this step, each party (KDC and publisher/subscriber) sends their own certificate and verifies the other certificate for validity as well as revocation status, by using Online Certificate Status Protocol (OCSP) (2'). Only if the verification succeeds, the KDC sends a Security Association (SA) including information on security algorithms for encryption, and integrity check. Devices (publisher/subscriber) send acknowledgement if they support the security algorithms mentioned in SA. Upon acceptance from devices, the KDC starts step 3, during which it sends the symmetric keys to devices. These keys are used for signing and, optionally encrypting the R-GOOSE.

Also the symmetric keys for data signing/encryption need to be updated at least once every two days, process called "rekeying". When this is done through the pull mechanism, each UR has to repeat step 2 and 3. There is also rekeying possible through the push mechanism, in which case KDC server sends the new keys to all members of the group usually in one multicast message. The KDC server is the one that decides when the keys will be changed.

VI. Summary

The GOOSE mechanism has already been used for protection and control applications over LANs. In order to use the GOOSE over WAN for WAPC applications, this paper presents implementation of IEC TR 61850-90-5 based on R-GOOSE protocol. High-speed (priority tagging), multicasting, and security mechanisms supported by R-GOOSE are described. R-GOOSE is compared to synchrophasor applications, network bandwidth, and performance requirements. Although there are pros and cons of synchrophasors and R-GOOSE approaches, both approaches can be implemented in the same system using IEC TR 61850-90-5-based synchrophasors (R-SV) and R-GOOSE. This approach takes advantage of best of both technologies. Furthermore, use case of SCE's project on Centralized-RAS using R-GOOSE is presented. Finally, the security mechanism implementation is described for R-GOOSE-based WAPC applications.

REFERENCES

[1] M. Begovic, D. Novosel, D. Karlsson, C. Henville, G. Michel, " Wide Area Protection and Emergency Control," in IEEE proceedings, vol. 93, no.5, pp. 876-891, May 2005.

[2] IEEE PES Power System Relaying Committee WG C4 report on, "Global Industry Experiences with System Integrity Protection Schemes (SIPS)," Oct. 2009

[3] IEEE PES Power System Relaying Committee WG C15 report on, "Design and Testing of Selected System Integrity Protection Schemes (SIPS)," Nov. 2012.

[4] IEC standard for Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasors information according to IEEE C37.118, IEC 61850-90-5, TR Ed 1.0, 2012.

[5] T. Sidhu, M. Kanabar, P. Parikh, "Configuration and Performance Testing of IEC 61850 GOOSE," Advanced Power System Automation and Protection (APAP), pp.1384-1389, Oct. 2011.

[6] A. Apostolov, B. Vandiver, " To GOOSE or Not to GOOSE? That is the question," PAC World Magazine, June 2015. Available: https://www.pacw.org/issue/june_2015_issue/cover_story/to_goose_or_not_to_goose_that_is_the_question/complete_article/1.html

[7] M. Yalla, M. Adamiak, et. al. "Application of Peer-to-Peer Communication for Protective Relaying," IEEE Trans. On Power Delivery, Apr. 2002.

[8] C. Wester, M. Adamiak, J. Vico "IEC61850 protocol - practical applications in industrial facilities," IEEE Industry Applications Society Annual Meeting, Oct. 2011

[9] RFC 3376 – IGMP version 3

[10] IEC 62351-9 – Data and Communication Security – Key Management, version 2 draft, containing R-GOOSE security requirements previously described in IEC 61850-90-5.

[11] RFC 6407 – The Group Domain of Interpretation (GDOI)

[12] GDOI Protocol Support for IEC 62351 Security Services (6th revision): http://www.ietf.org/id/draft-weis-gdoi-iec62351-9-06.txt

[13] IEEE Standard for Synchrophasors Data Transfer for Power Systems, IEEE C37.118.2, 2011.

[14] V. Madani, M. Kanabar, Y. Yin, F. Rahamatian, M. Adamiak, "Roadmap and Lessons in Deploying Large Scale Synchrophasor Systems," CIGRE US 2014 Grid of the Future Symposium, Houston, Texas, Oct. 2014.

[15] Y. Hu, R. M. Moraes, V. Madani and D. Novosel, "Requirements of Large-Scale Wide Area Monitoring, Protection and Control Systems," *Proc.* 10*th Annu. Fault Disturbance Anal. Conf.*, Atlanta, April 2007, pp. 1-9.

[16] J. Wen, P. Arons, "Implementation of Centralized Remedial Action Scheme – An Important Step towards WAMPAC," IEEE PES GM Smart Grid Super Session, July 2011.

[17] A. Johnson, J. Wen, J. Wang, E. Liu, Y. Hu, " Integrated System Architecture and Technology Roadmap toward WAMPAC," IEEE Smart Grid Technologies conf. Anaheim, USA, Jan. 2011.

[18] J. Wen, C. Hammond, E. A. Udren, "Wide-Area Ethernet Network Configuration for System Protection Messaging," in IEEE Proc. Texas A&M Conf for Protective Relay Engineers, Apr. 2012.

[19] GE Multilin – N60 Network stability and synchrophasor measurement system, GE Manual Publication – GEK-113387.

[20] H. Falk, "The anatomy of a Centralized Remedial Action System: what can be done in 50 milliseconds?" white paper by SISCO.

BIOGRAPHIES

M. Kanabar is a Lead Product R&D application engineer with GE-Grid Solutions. He received his B.E. degree from Sardar Patel University, Gujarat, India, in 2003. He was with Larsen and Toubro Ltd., India from 2003-2004. He received his M.Tech degree from Indian Institute of Technology (IIT) Bombay, India in 2007. He received his Ph.D. from the University of Western Ontario in 2011. Since then, he has been with GE Grid Solutions, working on the development of grid automation & protection solutions. Mital holds 6 international patents, and author of 30 journal/conference papers, and a book chapter. Currently, Mital is vice-chair of IEEE PES PSRC WG C19 and WG K15; and active member of technical WGs/TFs at IEC, NASPI, NERC and CIGRE.

Anca Cioraca is an Information Technology Professional with over twenty years hands on experience in system and software architecture, specialized in communications, networking and cybersecurity. Anca has a Master of Engineering degree in Electronics and Telecommunications from Bucharest Polytechnic University, Romania. In 1991 Anca moved to Canada and for the following twenty years she focused on software architecture and cyber security for network devices, such as routers, firewalls and security servers, while working for Motorola, Enterasys, Siemens and WatchGuard. In 2012 Anca joined GE Grid Solutions. Currently Anca leads the cyber security architecture for next generation GE Grid Solutions Grid Automation products. Anca is a member of IEEE Communications Society and the IEC TC57 working group WG15, where she actively contributes to the definition of security requirements for the TC 57 series of protocols.

A. Johnson, P.E. is a consulting engineer in Advanced Technology for Southern California Edison. In his present role, he collaborates with and directs a wide range of groups. Previously he led the Power System Studies Group, responsible for SCE special studies, providing technical expertise in control methodologies for static var compensators and the deployment of advanced technologies. Mr. Johnson earned his BS and MS in electrical engineering from Montana State University in 1986 and 1988 respectively, and has been with SCE for 25 years. He is a member of IEEE, and a registered professional electrical engineer in the State of California.