

Project title – Substation Automation

A)Background and Related work

A power substation network consists of tens or hundreds of microprocessor-based IEDs that control, monitor, and protect the power grid. An IED is usually equipped with one or more microprocessors, memory, possibly a hard disk and a collection of communication interfaces (e.g. USB ports, serial ports, Ethernet interfaces), which implies that it is essentially a computer as those for everyday use. Nowadays, IEDs are increasingly connected by Ethernet and use digital communication protocols for transmitting status data, control commands and configuration/maintenance information. IEC 61850 [19] is a specification for the design of substation automation that uses object- oriented data models to describe the information available from various primary equipments and substation automation functions. It also specifies the communication interfaces between IEDs and maps them to specific protocols. A typical IEC 61850 substation architecture is shown in Figure 1.

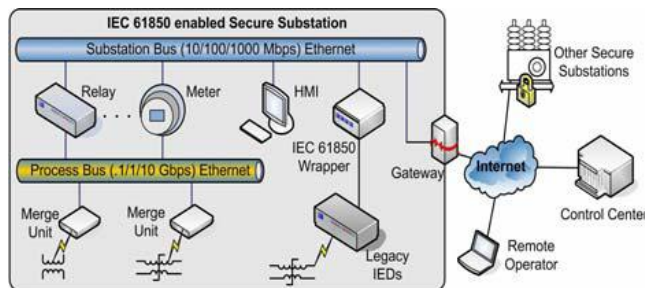


Figure 1: Typical substation architecture

The substation network is connected to the outside wide area network via a secure gateway. Outside remote operators and control centers can use the abstract communication service interface (ACSI) to query and control devices in the substation. There is one or more substation buses connecting all the IEDs inside a substation. A substation bus is realized as a medium bandwidth Ethernet network, which carries all ACSI requests/responses and generic substation events messages (GSE, including GOOSE and GSSE). There is another kind of bus called process bus for communication inside each bay. A process bus connects the IEDs to the traditional dumb devices (merge units, etc.) and is realized as a high bandwidth Ethernet network. A substation usually has only one global substation bus but multiple process buses, one for each bay. ACSI requests/responses, GSE messages and sampled analog values are the three major kinds of data active in the substation network. Interactions inside a substation automation system mainly fall into three categories: data gathering/setting, data monitoring/reporting and event logging. The former two kinds of interactions are the most important — in the IEC 61850 standard all inquiries and control activities towards physical devices are modeled as getting or setting the values of the corresponding data attributes, while data monitoring/reporting provides an efficient way to track the system status, so that control commands can be issued in a timely manner.

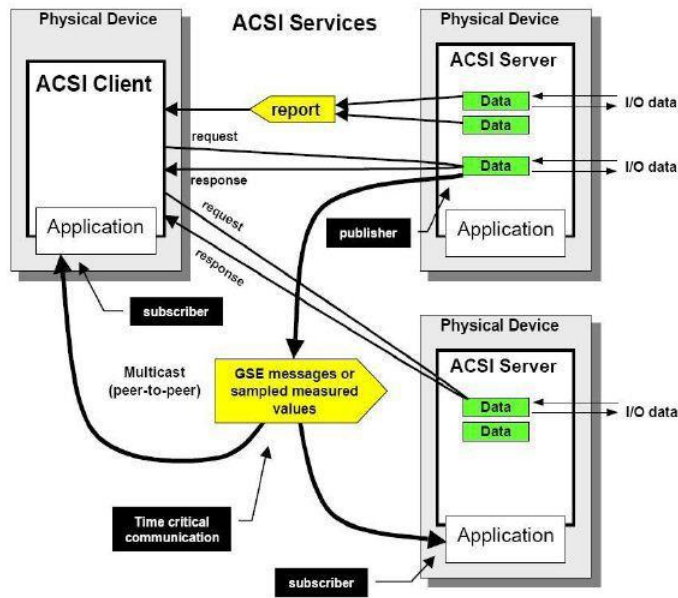


Figure2: ACSI Communication model

IEC 61850 consists of three major parts:

- An object data model describing the information available from different primary equipment types and from substation automation functions
- A specification of the communication interfaces between IEDs and the schemes mapping them to a number of protocols running over TCP/IP and high speed Ethernet.
- An XML based configuration language used for exchanging the power system, substation network and devices configuration information.

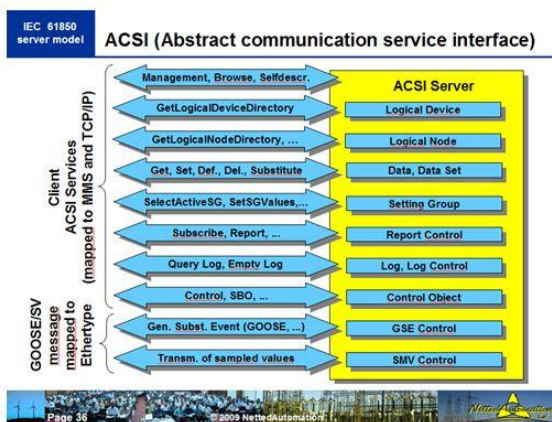


Figure 3 : IEC 61850 Server model

Substation Communication:

Abstract Communication Service Interface (ACSI) requests/responses, sampled analog values and GSE messages are three major kinds of data exchanged in IEC 61850 substation networks.

ACSI is designed for non timing-critical and client-server style message transmissions, including device configuration, maintenance, event logging and reporting. Sampled Measured Value (SMV) is an Ethernet link layer protocol used to periodically collect digitalized analog power data on the process bus. Generic

Substation Event (GSE) is designed for fast and reliable system-wide distribution of input and output data values. It has two major forms: Generic Object Oriented Substation Event (GOOSE) and Generic Substation State Event (GSSE). GOOSE is used for fast exchange of a wide range of common data or substation events organized in a data set. Both GOOSE and GSSE work in publisher-subscriber style and messages are transmitted by multicast. GOOSE is also an Ethernet link layer multicast protocol designed for timing-critical messages within substation networks via substation buses. It is used for transmitting substation events, commands and alarms, *etc.* Because GOOSE is directly mapped to Ethernet frames, it can take advantage of high speed switched Ethernet and is capable of fulfilling realtime requirements.

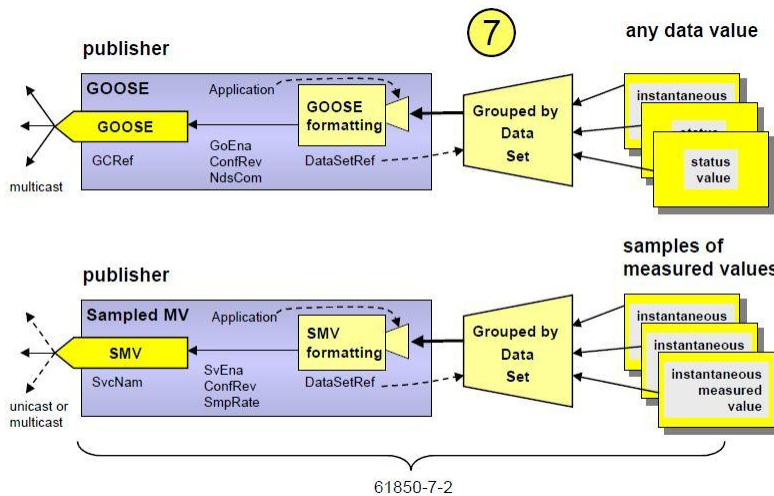
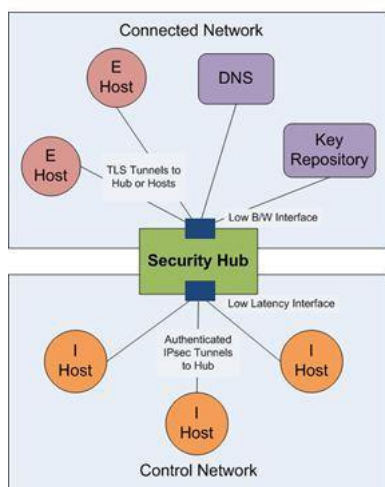


Figure4- Peer to Peer data publishing model

Event notification exchanges for protection within a substation must be transmitted within between 2 and 10 milliseconds. It is common to quote a benchmark of 4 milliseconds.

Security Hub Architecture -



A security hub [12] is a network element whose purpose is to provide broad access to a distinguished collection of hosts while assuring latency requirements between these distinguished hosts. The concept is illustrated in the figure. The security hub links two networks: a connected network such as the Internet or

enterprise network and a control network such as the digital communication bus in a power station. Hosts in the connected network are said to be external hosts (ehosts) whereas hosts in the control network are called internal hosts (ihosts). The security hub manages communication with each ihost so that a packet from an ehost to any ihost must pass through the hub and a packet from any ihost to any other ihost must pass through the hub. The security hub provides a —hub-and-spokes network architecture for the ihosts while also acting as a gateway between the ehosts and the ihosts. It provides a low bandwidth interface to the connected network and a low latency interface to the control network. The hub maintains IPsec-authenticated tunnels between itself and each of the ihosts and takes responsibility for checking the authenticity of the origin of any packet sent between ihosts. It routes packets from the connect network to the ihosts through these tunnels, but leaves their authentication to the ihosts, which use TLS to provide both authentication and encryption for these links. Each ihost is given a DNS name and a certificate with a private key bound to this name. These keys are managed by a key repository which is located in the connected network. The nodes use the Domain Name Server (DNS) to get IP addresses for routing, including routing within the control network. The hub provides multicast addresses and routing for use by the ihosts. An ihost can declare a new multicast address and other ihosts can subscribe to it. Finally, the hub keeps a repository of the names of all of the ihosts attached to it in the control network and is able to provide this list to hosts authorized to receive it. The hub is also able to enforce basic partitioning of the ihosts by being configured so to allowing only some communication between the ihosts, thereby implementing an analog of a VLAN. There is need to provide for secure multicast communications in which messages are authenticated and possibly even encrypted. One could use security technology such as the Internet Security Protocol (IPsec) to address this need, but there are two problems: (1) Due to increasing complexity of substation configurations and the complexity of IPsec configuration there is need to provide automation for security configuration and (2) the latency requirements of substation communications must not be burdened respected by security protocols. It is a discovered fact that a trivial implementation of point-to-point IPsec using a hub-and-spokes model is not efficient enough to maintain substation latencies[1].

Group key management is one of the most important components of secure multicast systems. Academic research suggests a number of group key schemes [20, 21, 22, 23, 24]. These sophisticated solutions aim at the groups where group members shuffle frequently. The efficiency and scalability are the main concerns for these systems. However, in power grid systems, especially power substation networks, multicast groups are comparatively stable and the network scale is usually of medium size. Once the system design is finished, the network topology is rarely changed. In [25] and [26], researchers propose two very similar centralized group key management models. Both models introduce a group control and key server (GCKS) to manage group members and distribute/refresh group keys to group members. These two models are the bases for the GDOI [27]. Taking advantage of GDOI and directing the group authorization and group policy configuration by application logic is studied by Jianqing zhang in [1]. It also studies the feasibility of IPsec based multicast in power grid systems. Role of security hub as group key manager and distributor is discussed in [12]. Group key management by observation of group dynamics will be the first work in this area.

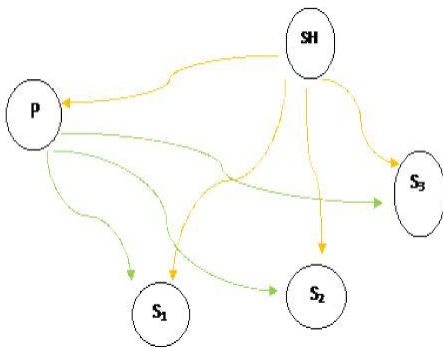




Figure 5 Group Control + Management Via Security Hub

-  Group Control + Key Management Flow
 Data Flow

Though a lot of work has been in network component of substation, very little study has been conducted in effectively modeling information model of IEC 61850 like database security and its efficient prototype modeling in resource constrained environments, issues like memory management. Study of latency problems at database level in IEC 61850 prototype, issues like fast record insertion, querying will be first work in this area. Also, much efforts has been concentrated in reducing latency by using efficient security protocols like IPsec as in [1], but very little work has been in reducing latency at kernel level by efficient packet generation techniques. Bypassing layers using raw sockets for GOOSE messages will an original work in this area.

Intrusion detection and security analysis in Power grid is also a challenging task. Traditional ICT security technologies are not able (as illustrated in [1]) to effectively protect industrial systems against ad-hoc SCADA-tailored attacks. A novel approach for detecting ICT attacks on Power systems based on the concept of critical state analysis will be an interesting area[28]. By observing the dynamics of the grid process states, and tracking down when the industrial process is entering into a critical state, it would be possible to detect particular attack patterns (known or unknown) which plan to put the process system into a known critical state by using chains of licit commands. Also, the security status of any given operating condition can be classified into four modes namely secure, critically secure, insecure, and highly insecure, based on the computation of a security index. The classification of the system static/transient security status in multiclass domain gives an indication of security level to the system operator and helps to initiate necessary control actions at the appropriate time, preventing system collapse. A multiclass support vector machine (SVM) classifier for static and transient security assessment and classification can be worth intriguing[29]. Also, determination of a metric scheme to perform a security audit on a sample IEC61850 network can be challenging [30].

B) Research Questions –

IEC 61850 server is the most important component of substation network. Its efficiency is essential for smooth functioning of substation. Data stored in IEC 61850 servers is critical. Failure to retrieve data values from the database, set values in the database can disrupt the entire functioning of substation and can result in catastrophe. IEC 61850 server should meet strict real time requirements. IEC 61850 has to handle transactions quickly, query, retrieving times from the database should be lowest possible. Moreover, server has to operate in resource constrained environments.

This lead to some fundamental questions –

How to maintain efficiency of IEC 61850 server? How to make sure it has minimum downtime ?

This lead to some questions such as how to minimize insertion and retrieval times of records in IEC 61850 Database? how to take efficient back up of data stored in IEC 61850 server? How to recover IEC 61850 server quickly in case of crash? How to effectively manage memory occupied by database in IEC 61850 server?

Transmission of GOOSE/SMV messages in a substation has to meet strict latency requirements. TRIP command to circuit breakers has to meet strict latency requirement of 4 milliseconds. Moreover, security should be implemented on top of it. Thus security protocols such as IPsec adds to additional overhead. Efficient generation of GOOSE AND SMV packets is a must.

This leads to some fundamental research questions –

How to generate GOOSE and SMV packets quickly and efficiently? How and which headers to avoid during packet construction?

As GOOSE and SMV message adopt multicast application association and follow publish /subscribe mechanism, there is generation of multicast groups. These GOOSE and SMV messages must be transmitted in a secure manner. Thus, principles of secure group communication must be applied. As, environment is resource and time constrained, this lead to foremost question?

How to efficiently manage keys? How to minimize key generation and key transmission messages? How to implement efficient rekeying? How to implement source of efficient key back up which can be queried within substation network transparently?

Intrusion detection on a network and host level can be considered as a viable security countermeasure for IEC 61850 networks. Some questions which arise are –

How to detect when attack patterns are unknown ? How to detect on the basis of system evolution rather than on the basis of attack evolution? How to prevent zero day attacks?

Also, how to do a security audit on a time critical IEC 61850 enabled substation network? How to devise operating conditions classifier which can classify operating conditions into security levels such as secure, insecure, highly secure which can then issue appropriate alerts to the operator to prevent catastrophes?

C) Methodology -

1) IEC 61850 Prototype - Database Issues

Data values have to be fetched from IEC 61850 database. This needs database to reside in main memory to save latencies involved in fetching the data from the disk. A real time main memory resident database should be used in IEC 61850 prototype. In order to minimize memory occupied by database, dynamic allocation of database records is a must. Use of TLSF Dynamic Memory allocator suitable for real time purposes is proposed. TLSF results in $O(1)$ memory allocation and deallocation for records which helps in fast record creation.

Now, IEC 61850 database should recover quickly in case of crash. This involves categorization of data according to back up priority (For eg- Temporal and Persistent). Data and data attribute records are changed pretty frequently so they can be backed up at a much higher rate than persistent data such as logical node and device information. Scheduling backup by efficient checkpointing. A Reload threshold can be set such as when certain segments of database image is loaded in memory, database can start operating and processing transactions or service commands. This feature enables fast recovery. In this regard certain experiments should be designed such as studying loading times of database as a function of database size.

2) IEC 61850 Prototype – Network Interface Issues

Construction of GOOSE/SMV Packets :

Use of raw sockets to create custom SMV, GOOSE messages. For Eg. GOOSE packets can be constructed using raw sockets by putting together data and Ethernet header. Exploring issues related to latencies at socket level.

3) Enabling Group Control and Management in Substation networks.

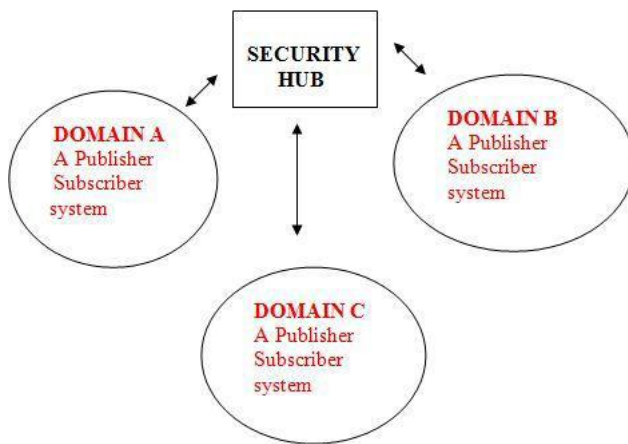
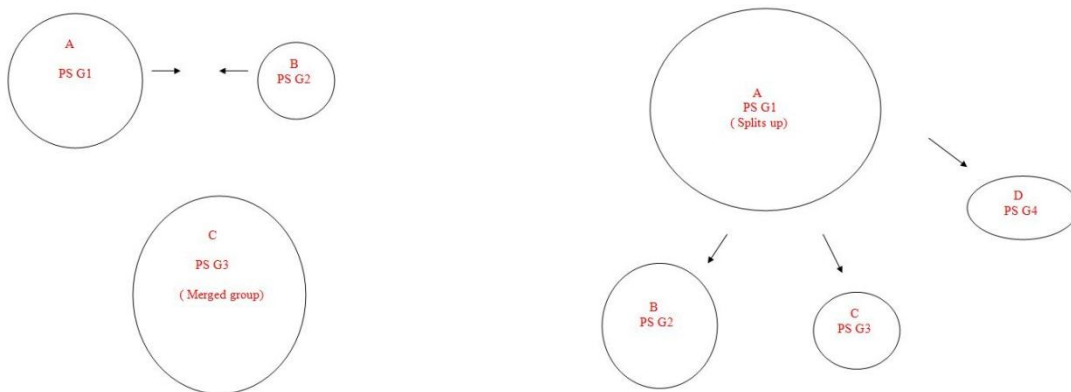
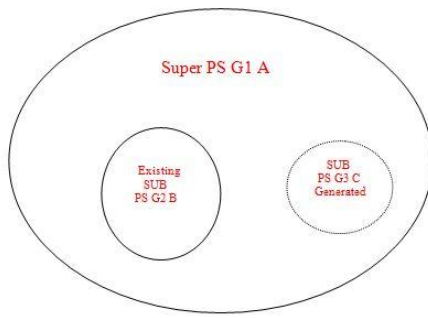


Figure 6. Publisher/Subscriber groups operating in a substation network



(a) Group Merge

(b) Group Split



(c) Subdomain generation

Figure 7. Group Dynamics models

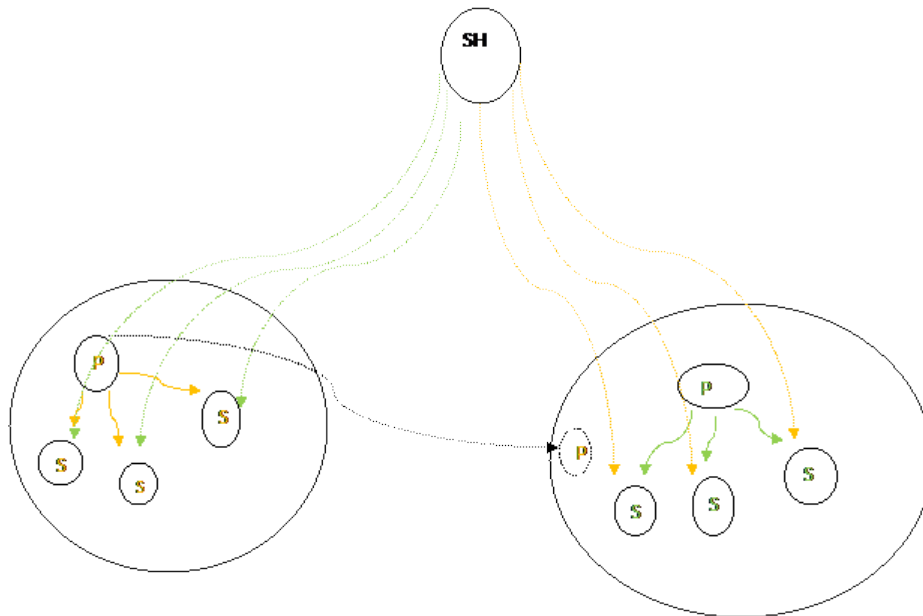


Figure 8. Example of transmission of rekey messages in case of domain merge via Security Hub

- Publisher/Subscriber group in Domain A
- Publisher/Subscriber group in Domain B
- ⋯→ Rekey Messages sent from Security Hub to Subscribers of domain A
(Only group key and pairwise session keys between members of domain A and B needs to be sent)
- ⋯→ Rekey Messages sent from Security Hub to Subscribers of domain B
(Only group key and pairwise session keys between members of domain A and B needs to be sent)

Effect on key distribution-

Eg- In case of a domain merge-

A new group key is generated for new group. Also, pairwise session keys are generated between members in domain1 and domain2 respectively. Suppose there are 'a' members in domain1 and 'b' members in domain2. So, total no. of session keys to be generated 'ab'. Each member in domain A receives b+1 keys ('b' pairwise session keys + 1 group key) and unicast message for domain B members contains a+1 keys ('a' pairwise session keys + 1 group key). Total no. of unicasts a+b. In absence of dynamics- No. of keys to be generated $^{a+b}C_2$ pairwise session keys + a group key.

Key Management is an important issue in resource constrained environments. Use of key graphs and observations of group dynamics can have significant impact on rekeying operations. Such logic can be implemented within the security hub as part of group control and key management application. Security hub can also acts as a source of key backup. Also, replication of security hub in the control network might enhance reliability and performance.

Study of factors which may be leading to group dynamics (if present) in substation publish/subscribe groups can be an interesting area. Factors can be subscribers receiving messages from IEDs which are functionally related. Study if publisher/subscriber group formation behavior in substation IEDs is dependant upon time. Give a time series if possible for various group dynamics models like coalesce, split etc. Do time series analysis, forecasting. Find anomalies in group dynamics behavior using time series discords. If possible, develop a simulator program illustrating behavior of publisher/subscriber groups in a substation.

4) Intrusion detection in power grid networks is a challenging task. Approach based on the concept of Critical State Analysis and State Proximity is highly innovative[28]. Proposed IDS keeps will keep track of the chain of packets driving the system into a critical state (storing details about such packets in a remote database and using the Critical State Distance Metric as trigger for logging a chain of packets). It can help in detecting particular types of Substation attacks based on chains of licit commands. It will include modelling the following in a IEC 61850 enabled substation environment–

- A *system representation language* to describe in a formal way the system under analysis.
- A *system state language* to describe in a formal way the critical states associated to the system under analysis.
- A *state evolution monitor* to follow the evolution of the system.
- A *critical state detector* to check whether the state of the system is evolving toward a defined critical state.
- A *critical state distance metric* to compute how close any state is with respect to the critical states.

Such Detection will be based on evolution of a system rather than attack evolution.

Also, an Event correlator engine can be built which can co-relate series of event driving system into critical states. Critical states can be grouped into categories such as similar, partially similar and diverse. This will lead to more efficient and detailed diagnosis. We could also consider techniques such as deterministic finite automata used to create flow models to depict system evolution ,and Markov models and find relationships in system evolution.

D) Research Plan and Timeline –

Phase 1 –

- Study of IEC 61850 server database issues and issues related to database security and efficiency.
- Implementation of IEC 61850 server compliant with these requirements

Phase 2 –

- Study of efficient packet construction for GOOSE/SMV
- Implementation of same using RAW sockets
- Study , how it can be combined with efficient security solutions
- Do, we achieve the goal of meeting latency requirements with security requirements ?

Phase 3 –

- Study of key management and group control in resource constrained environments
- Implementation of key management solutions such as group dynamics within substation network.
For eg – Using Security Hub

Phase 4 –

- Develop intrusion detection system based on Critical State Analysis and State Proximity for substation

Combining these essential components of substation, we studied during three years and figuring out whether a better and secure model of substation automation has been achieved.

E)References :

1)*Secure Multicast for Power grid communications*

Jianqing Zhang. Doctoral Thesis, University of Illinois, September 2010.

2)*Application-Aware Secure Multicast for Power Grid Communications*

Jianqing Zhang, Carl A. Gunter. The 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, MD. October 2010

3)*On the Latency of IPsec Multicast in Power Substation Local Area Networks*

Jianqing Zhang, Carl A. Gunter. Manuscript, Urbana, IL. June 2009

4)*Evaluating A Secure Protocol Scheme for Control Networks on the DETER Test Bed*

Jianqing Zhang, Carl A. Gunter. Manuscript, Urbana, IL. June 2008

5)*The Protection of Substation Communication*

S Fuloria, R Anderson, K McGrath, K Hansen, F Alvarez. In proc. of SCADA Security Scientific Symposium, Jan 2010

6)*Key Management for Substations: Symmetric Keys, Public Keys or No Keys?*

S Fuloria, R Anderson, Fernando Alvarez, K McGrath. PSCE 2011: the IEEE Power Systems Conference & Exposition, March 2011, Phoenix, Arizona, USA

7)*TLSF: A New Dynamic Memory Allocator for Real-Time Systems*

M. Masmano, I. Ripoll, A. Crespo and J. Real. 16th Euromicro Conference on Real-Time Systems (ECRTS 2004)

8)Boost socket performance on Linux : <http://www.ibm.com/developerworks/linux/library/l-hisock.html>

9)<http://blog.iec61850.com/search?updated-min=2011-01-01T00:00:00-08:00&updated-max=2012-01-01T00:00:00-08:00&max-results=26>

10)<http://www.lams.cl/libreria/IEC%2061850%20Network%20Architectures.pdf>

11)<http://iec61850.blogspot.com/>

12)*Security Hub Architecture support for IEC 61850 information exchange protocols*

Suhas Aggarwal. Accepted at: The 4th IASTED Asian Conference on Power and Energy Systems (AsiaPES 2010), Phuket, Thailand

13)*IEC 61850 : Prototype Design*

Suhas Aggarwal. Accepted at : 2nd IEEE PES Innovative Smart Grid Technologies Conference (ISGT 2011), Anaheim, CA USA

14)Cheetah – IEC 61850 server code available at –

<http://sites.google.com/site/suhasprojectprofilesite/sieds-2>

15) *A Soap Bubble Model for Coalescence, Rearrangement, and Splitting Reactions of Fullerenes*

Takayuki Ohmae

16) Experiments on Droplet Collisions, Bounce, Coalescence and Disruption

Melissa Orme

17)*Finding the Unusual Medical Time Series: Algorithms and Applications.*

Keogh, E. , Lin, J., Fu, A. & Van Herie, H. *IEEE Transactions on Information Technology in Biomedicine* (2005).

- 18) http://www.scc-online.de/std/61850/documents/61850-7-1_R2-05_FDIS_To-IEC-CO_2002-11-04.pdf
- 19) IEC TC 57/WG 10-12, “IEC61850 Communication Networks And Systems In Substations,” April 2003.
- 20) *Key Management For Secure Internet Multicast Using Boolean Function Minimization Techniques*
I. Chang, R. Engel, D. Kandlur, D. Pendarakis, and D. Saha.. In 8th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM’99), March 1999.
- 21) *Scalable Secure Group Communication Over IP Multicast*
S. Banerjee and B. Bhattacharjee.. Selected Areas in Communications, IEEE Journal on, 20(8):1511 – 1527, October 2002.
- 22) *Secure Spread: An Integrated Architecture for Secure Group Communication*
Y. Amir, C. Nita-Rotaru, J. Stanton, and G. Tsudik.. IEEE Transactions on Dependable and Secure Computing, 2(3):248 –261, July 2005.
- 23) *Key Establishment in Large Dynamic Groups Using One-Way Function Trees*
A.T. Sherman and D.A. McGrew.. IEEE Transactions on Software Engineering, 29(5):444–458, 2003.
- 24) *Secure Group Communications Using Key Graphs*
C. K.Wong, M. Gouda, and S. S. Lam.. IEEE/ACM Transactions on Networking, 8(1):16 –30, February 2000
- 25) *The Multicast Group Security Architecture*
T. Hardjono and B.Weis.. RFC 3740 (Informational), Mar.2004.
- 26) *Multicast Security (MSEC) Group Key Management Architecture*
M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm.. RFC 4046, Apr. 2005.
- 27) *The Group Domain of Interpretation*
M. Baugher, B. Weis, T. Hardjono, and H. Harney. RFC3547, July 2003.
- 28) *A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems*
Andrea Carcano, A. Coletta, Michele Guglielmi, Marcelo Masera, Igor Nai Fovino, Alberto Trombetta, IEEE Trans. Industrial Informatics 7(2): 179-186 (2011)
- 29) *Classification and Assessment of Power System Security Using Multiclass SVM*
Kalyani, S., Shanti Swarup, K., IEEE Trans. On Systems, man and cybernetics
- 30) *Security Analysis and Auditing of IEC61850 Based Automated Substations*
U. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. C. Tan, ,” IEEE Trans. On Power Delivery, Vol. 25, Issue 4, 2010, pp. 2346 - 2355.
- 31) *An Event Correlation Approach for Fault Diagnosis in SCADA Infrastructures*
Massimo Ficco, Alessandro Daidone, Luigi Coppolino, Luigi Romano and Andrea Bondavalli.
EWDC '11 Proceedings of the 13th European Workshop on Dependable Computing
- 32) *Intrusion detection in SCADA networks*
Barbosa, Rafael Ramos Regis and Pras, Aiko ,4th International Conference on Autonomous Infrastructure, Management and Security, AIMS 2010, June 23-25, 2010, Zurich, Switzerland.