System Architecture and Security Overview for Smart Grids

Philani Khumalo
Electronic Engineering Department
DUT, Steve Biko campus
KhumaloPK@elec.durban.gov.za

B. Nleya
Department of Electronic Engineering
DUT, Steve Biko Campus
bmnleya@gmail.com

***Abstract*—The Smart Grid approach is geared towards improving power supply efficiency as well as reliability of existing power grid systems by modernizing them with Information and Communication Technologies. Despite its promising as well as already attractive features, it remains vulnerable to security threats and as such these should be adequately addressed. In this paper we review, system architecture for the smart grid as well as security and access control requirements. In particular, it is noted that the complex structure of a Smart Grid, implies management complexities, mainly due to the different power generating sources which lead to complex management due to the multitudes of data exchanges involved.**

Keywords— Smart Grids, access control, smart meters

I. INTRODUCTION

A Smart Grid (SG) is the new version native power system grid that adopts Information and Communication Technologies (ICT) to enhance overall efficiency and reliability of power grid system. [1]. Traditionally, most power generating systems have always relied on fossil fuels. However, because of the latter's fast depletion as well as environmental unfriendliness, there is a gradual attention towards renewable energy sources to replace them. Renewable energy sources such as wind and solar generate power intermittently, i.e. solar powered electric generating systems rely on the sun hence generate electricity during daylight times only. It is thus vital that new generation power grid management systems be developed to cope with associated challenges. In a way, the smart grid is a promising solution towards the integrating and availing of renewable resources to the existing power grid and an ideal platform for power users to participate in the electricity enterprise. A typical SG incorporates several layers (figure 1) that include; a power system layer that encompasses distributed power generation, transmission, distribution as well as consumer systems; a power control layer, that monitors and controls the entire smart grid; a communication layer, which facilitates semi duplex data exchange within the smart grid environment; a security layer, which ensures data integrity, confidentiality, authentication as well as availability; and finally an application layer, which facilitates various innovative smart grid applications to power users and utilities, a key example being advanced metering infrastructure (AMI) which is a key application in the realizing of a SG. The communication layer is one of the most critical elements that enables smart grid applications. Various entities/functionalities contribute to overall data that is exchanged within the SG. Examples include:

The Phasor Measurement Unit: which dedicates towards providing synchronized phasor measurements of key quantizes such as voltages and currents in the power grid. It does so by way of sampling these quantities waveforms using a common synchronizing sampling signal tapped from Global Positioning Satellite (GPS) system. Typically, the reporting is fixed at 20 to 50Hz. Each power utility will generally have a centralized, Phasor Data Concentrator (PDC) for aggregating and aligning data from several PMUs within the SG before relaying it to a central facility where synchronization network wide is accomplished [2].

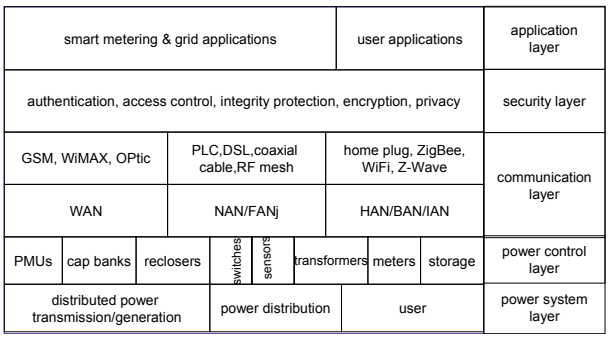

Figure 1. Smart Grid multi-layer [1]

Standard IEEE Std C37.118-2005 defines four message types for PMUs output as data, configuration, header, and command [3]. Typically, each message is 100~200 bytes. Overall transmission latency is bounded to 10~20 microseconds or less [3].

As mentioned earlier, smart meters manage, monitor and control power supply to the end users, and in some instances, can also relay data to and from gateway smart meters [4]. The gateway smart meters, in turn, relay the collected data to control centers of utility companies to support the pricing and decision-making. In short, not all smart meters (nodes) can communicate with the collector directly. Intermediate smart meters cooperate in relaying data packets on behalf of one

another until the data packets reach the gateway smart meter. This procedure is called data aggregation (figure 2).

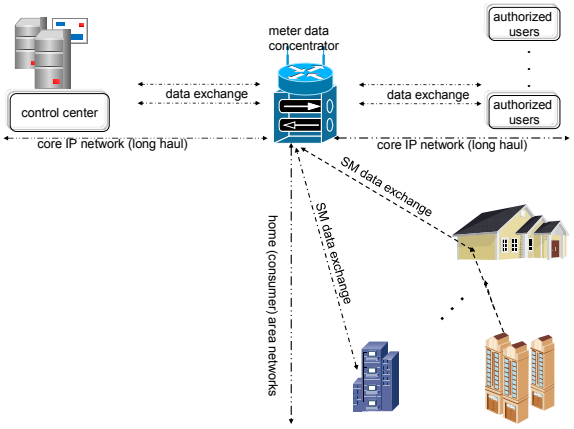

Figure 2. Smart meter Data Aggregation

Typically, we have home area networks (HANs), and building area networks (BANs). HANs collect information and send it via neighbor BANs. Ultimately all the information from smart meters is aggregated at a local substation, where a remote terminal unit (RTU) finally sends the aggregated data to a gateway smart meter. The gateway smart meters associated with each RTU finally send aggregated results to data centers, from which the information is distributed to users for maintenance, auditing, future predictions etc.

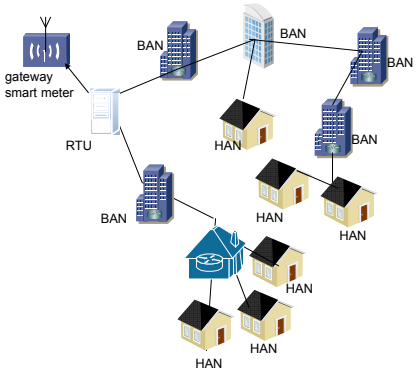

Figure 3. Data collection.

Data in transit becomes vulnerable in that, intermediate nodes can place the data at security risk without being detected by the core smart grid and thus it is important to secure the smart grid. As cited earlier, the information from RTUs at the substation is crucial for key management purposes such as power distribution, cost accounting, as well as future grid behavior predictions.

Ideally, a security architecture that ensures privacy during both large-scale data aggregation as well as access is desirable. Large scale data aggregation will require efficient data aggregation trees as well as reliable encryption key distribution for access control. A policy based encryption scheme for access control in smart grids was proposed in [5] with the assumption of the existence of a reliable and honest key distribution center (KDC) that distributes keys and access policies to data senders and receivers, who in turn can only decipher information, if they have a valid set of attributes. For reasons of efficiency, reliability and security, multiple KDCs connected in a distributed fashion would be desirable (figure 4.

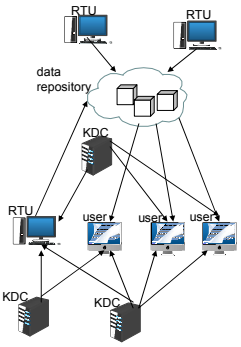

Figure 4. KDC connected in a Distributed fashion

II. SMART GRID SECURTTY OVERVIEW

Security mechanisms in Smart Grids must be applied at both physical and logical layers. At physical layer level, all key smart grid components and systems must be protected from theft, harm, tempering as well as general sabotage. At the logical layer levels, data semantics would be the focus. Summarily key logical layer security mechanisms desirables include:

- *Encryption*. Data exchange(s) between smart meters and utility centers must be secured from snooping, hence preserving its confidentiality. Robust but efficient encryption algorithms are desirable in this case. This calls for all key smart grid elements such as collectors, mart meters, routers and processors to be enabled with encryption processing capabilities.
- *Application Security Controls*. All Smart Grid applications should be designed and implemented in such a way that e.g., cyber criminals may not be able to easily access an element to embed a malware or even mount buffer overflow attacks.
- *Malware Removal*. capability to use antispyware and antivirus software throughout the smart grid applications should be provisioned to help detect and remove any malwares from the smart grid system.
- *Authentication*. Key Smart grid applications should have accurate and strong authentication capabilities, to seclude any possible unauthorized connections to any of the grid's components.
- *Security Patches*. It can protect an application from known threats; therefore, codes should be kept up to date with latest security patches.

Overall, ensuring cyber security in smart grid requires real-time monitoring and control so that any possible security violation can be expeditiously detected and appropriate remedial actions taken quickly. Furthermore, monitoring all key smart grid parameters can assist in quickly identifying any abnormal or suspicious activities.

III ACCESS CONTROL IN FEDERATED SG DATA CLOUDS

In this section, we describe a possible access control in Federated Smart Grid Clouds. By "federated Clouds', this refers to the management of a user's access rights or identity across different Smart Grids or microgrids. Note that the cloud federation can be at microgrid or SG to SG levels. Usually a user is authenticated in one Smart Grid domain.

A: Access Control Architecture

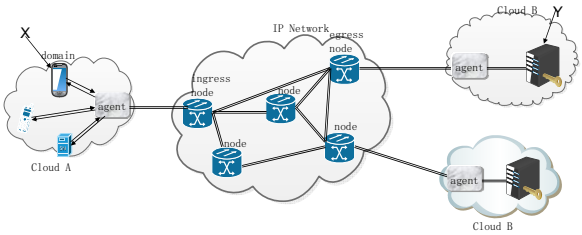

Figure 5. Federated Cloud access control architecture

The proposed access control architecture is illustrated in fig 6. Each federal domain. Each domain has an Agent Unit to which all devices and components are connected [7]. The domain is also connected to the IP backbone network. Features characterizing the architecture include authentication for each user's access request (s) as well as a QoS secure path selection. The authentication network is decentralized and hence each domain handles authentication requests from all its devices and components. High bandwidth end-to end authentication channels are logically separated from encrypted and QoS ensured data channels.

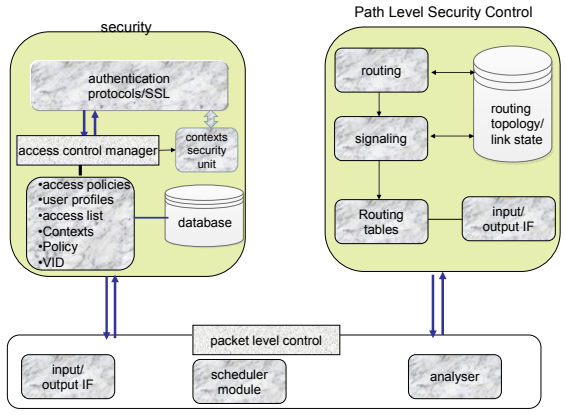

Figure 6. Agent Unit functionalities

The packet level control consists of an input/output interface. Upon reception of a packet, the analyzer unit differentiates access *request*, *data* or *control* packets by studying the service identifier field (ID). Any received authentication packet is passed on to the Security Block. Within this block, the Access Control manager (ACM) together with a set of authentication/SSL protocols [8] will negotiate for the desired access to a requested resources(s). under the coordination of the contexts security unit (CSU).

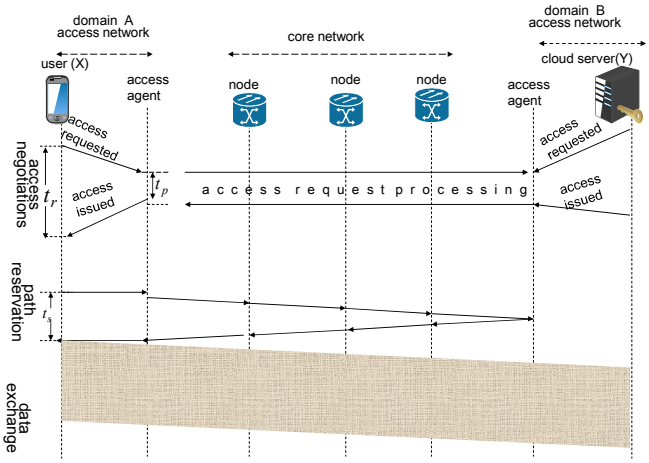

Figure 7. Message exchanges in authentication, channel reservation and data exchange processes

After the access is granted, an authentication notification in the form of a ticket is issued to the user. In a way, the CSU is a central point for security decisions. The control packet will also be used by the Path Level Security Control block in setting setup an encrypted path between the ingress and egress nodes. In so doing it uses the routing topology /link state database. The path selection is based on random routing shortest path first. The explicit route information i.e. the set of nodes to be traversed as well as required resources is now incorporated in the signaled from the ingress node to the egress node over a secure and dedicated control(signaling) and ultimately in the process reserving the requested secure path between the Agents. A summary message exchanges in authentication, channel reservation and data exchange processes is illustrated in figure 7.

IV. CONCLUSION

Whereas the architectural and related issues discussed earlier point to a realistic as well as feasible practical realization of the Smart Grids, a significant research effort is still required in order to address various issues including technology, standardization, security and privacy.

A full comprehension of industry and technology requirements and characteristics as a function of factors such as security, privacy, risk and cost is required before general acceptance of standardized deployment of Smart Grids. Core security and privacy approaches. also require further enhancements. Whereas existing network security protocols and related technologies provide a basis for privacy and security in Smart Grids, further improvements are still necessary.

REFERENCES

[1] W. Wang and Y. Xu and M. Khanna, "A survey on the communication architectures in smart grid", Computer Networks, (2011) July, pp. 3604-3629

[2] V. C. Gungor, D. Sahin, T. Kocak and S. Ergut, "Smart Grid Technologies; Communication Technologies and Standards", IEEE Transaction Industrial Information, vol. 7, no. 4, (2011), pp. 529-539.

[3] Xinxin Fan and Guang Gong. Security Challenges in Smart-Grid Metering and Control Systems. Technology Innovation Management Review, July 2013.

[4] Thsepiso Mooketsi, Nleya B and Andrew Mutsvangwa. Security Considerations foy Hybrid Smart Grids. IEEE PES 2016. Livingstone, Zambia, 28-30 June, 2016.

[5] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems (reprint)," Commun. ACM, vol. 26, no. 1, pp. 96–99, 1983.

[6] M. Chase, "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, S. P. Vadhan, Ed., vol. 4392. Springer, 2007, pp. 515–534.

[7] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in ACM Conference on Computer and Communications Security, ACM, 2009, pp. 121–130.

[8] Kazuhito Sagara, Kenya Nishiki and Minoru Koizumi. A Distributed Authentication Platform Architecture for Peer-TO-Peer Applications. IEICE Transactions on Communications, Volume E88, Number 3, March, 2005.

[9] T. Elgamul. The Secure Sockets Layer Protocol.(SSL). http://www.ietf.org/proceedings/95Apr/sec/cat.elgamal.slides.html, April, 1995.

[10] Guangdong Bai, Lin Yan, Liang Gu, Yao Guo, and Xiangqun Chen. Context-aware usage control for web of things. Security and Communication Networks, 2012.