A Taxonomy on Accountability and Privacy Issues in Smart Grids

Ameya Naik and Hamid Shahnasser
Electrical & Computer Engineering Program, San Francisco State University, San Francisco, U.S.A
Email: ameyunaik@gmail.com;

Abstract - Cyber-Physical Systems (CPS) are combinations of computation, networking, and physical processes. Embedded computers and networks monitor control the physical processes, which affect computations and vice versa. Two applications of cyber physical systems include health-care and smart grid. In this paper, we have considered privacy aspects of cyber-physical system applicable to smart grid. Smart grid in collaboration with different stockholders can help in the improvement of power generation, communication, circulation and consumption. The proper management with monitoring feature by customers and utility of energy usage can be done through proper transmission and electricity flow; however cyber vulnerability could be increased due to an increased assimilation and linkage. This paper discusses various frameworks and architectures proposed for achieving accountability in smart grids by addressing privacy issues in Advance Metering Infrastructure (AMI). This paper also highlights additional work needed for accountability in more precise specifications such as uncertainty or ambiguity, indistinct, unmanageability, and undetectably.

1. Introduction
The swift developments in technology along with the improvement and upgradation in physical systems have emerged into integrative and multi-faceted engineering systems called Cyber-Physical System (CPS). This system relies on collecting data for making controlled decisions for the physical system and managing communication. Smart grid is a good example for the Cyber-Physical System. Smart grid is a promising power delivery infrastructure incorporated with communication network and information technologies. Its main objective being improvement in power system, checking the transmission, distribution and consumption and its various collaborations to aid the consumer sector. With an upgraded sensing and control technologies, CPS can help in analyzing and determination of power usage, delivery and generation in a real-time. CPS can also be used to enhance proper assimilation of energy resources being distributed and the use of intelligent appliance control for boosting the energy efficiency. [1]
Also, to protect and overcome problems arising on the aspects of privacy, honor and confidentiality, accountability is required. Jing Liu and Yang Xiao [2] describe accountability as a system that is recordable and noticeable, thus making it legally answerable to communication principles for its actions. If security issues arise, the in-built accountability mechanism will play an integral role in investigating who is responsible for it. Thereby, once the problem has been identified, a pre-defined
program can be used to fix it automatically or it can be also resolved by releasing relevant information to experts for evaluation. [2]

2. Accountability and Authentication

“Accountability logic” is considered as most appropriate way to analyze the accountability of a secure system. Most of accountability logic structured for e- transactions. The usage accountability is critical to minimize and prevent power theft and in promotion of the billing. Thus, the user is responsible for demanding the amount of electricity and is billed with respect to his usage value. Moreover, the utility can help keeping a track of amount of electricity used by an individual compared to that of bulk energy.

Authentication plays a very important role in analysis of accountability. Since time-critical applications require proofs that guarantee the temporal activities of each principal, Kailar’s accountability logic can be extended to analyze such applications with logic for e-commerce protocols such as payment and public key distribution. He defined accountability as a property wherein unique identification of original client can be associated with an object or can be verified with third party. [3]

Although Kailar’s accountability logic allows some temporal context, which must be added to represent the validation period of security-related information, such as a time-critical aspect, M. Kudo [4] expands the Kailar’s logic so that it could represent temporal accountability. He emphasized on different kind of attacks on temporal records of payment times and an error that could occur during closing time of electronic submission. For this type of attack, a third-party architecture can be introduced for security.

Based on Kudo’s secure electronic submission protocol, accountability logic has been developed in home area network (HAN) of smart grid. Jing Liu, Yang Xiao and Jingcheng Gao [5, 6] jointly proposed a possible architectural framework for implementation of accountability logic and identification potential security problems in home area network (HAN) and Neighborhood Area Network (NAN). Based on communication capability, electrical appliances are divided into two categories: the smart appliances and the other regular appliances.

Jing Liu, Yang Xiao and Jingcheng Gao [5,6] proposed the protocol that addresses both power usage and real-time market price change issues. Focusing on the privacy concern of the client, an ideal meter should not disclose any information to unauthorized or unapproved requests. Adopting pseudonym mechanism in NAN, communication flow will become anonymous. Thus, systems are responsible in setting up of various witnesses to screen activities in observation process of an object. Once a variation in conduct is identified, those witnesses will give significant proof with a specific end goal to bolster their discoveries.

M. Stegelmann et al. [7] proposed a scheme, in which a smart meter transmits the valuable metering data to neighborhood aggregator. This aggregator applies anonymous protocol and resends the information to service providers. The information sent for billing is not anonymous but the same one is anonymous for service providers.

X. Lin [8] presents a routing protocol system with a secured protocol for ad-hoc network. This protocol enables secrecy of the source, destination and path. In this protocol, a source starts initializing the path request number and broadcasts it. This request consists of sequence number of the path and an encrypted destination address. The nodes in channel rebroadcasts the path requests after noting it. The destination responds back the path request and these nodes along the channel are reserved by checking and matching the information about several iterations like previous hops and next hops.
3. Privacy Analysis

Security and privacy are not the same. Security of data is critical with regards to smart metering. As the data is traded over open systems, it is defenseless to being seen or altered in its transmission by unintended individuals and this could have unfortunate outcomes for the people to whom the data belongs. Some of the privacy concerns resulting from smart metering systems, Attacker models, and potential security attacks on smart metering systems are:

3.1. Software vulnerabilities:
These Issues can occur at programming level that can leave a Framework open to attack. This could be an Operating System (OS) on a modern controller, or attack on firmware in a security gadget, or a zero-day powerlessness on a server working framework.

3.2. Hardware vulnerabilities:
This refers to physical hardware installed in the network. The basic purpose of hardware will be in the product which runs it, i.e. the firmware. Attack on firmware can be serious as it can make the remote gadgets which run the firmware useless. These firmware usages can be redesigned remotely over a system. If this firmware updated is initiated deliberately with malevolent or incorrect code it can possibly "block" the gadget, making it useless. This could bring about extreme downtime for whatever framework it relates to.

3.3. Network vulnerabilities:
Security of network systems is very important. Basic frameworks need to be set up in disconnected systems with constrained user access. Any entrance or departure to these frameworks need to be secured by vigorously fortified firewalls with strict access control instruments. Lower level frameworks, for example, production network needs utmost care and should be secured with firewall, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) and conceivably some 'hacker trap' frameworks should be introduced. WAN access to production network need to be constrained and very secured. Remote destinations and remote clients also should be secured and strict IPSec VPNs, or stay on private systems should be implemented.

3.4. Infrastructure/Server vulnerabilities:
This refers to bad setup in infrastructure of Information Technology (IT) frameworks, for example, setting all clients up with the same passwords, or passwords considering their name, and so on are extremely risky. Unpatched server vulnerabilities, especially those in view of the edge of a system or in a 'Neutral territory' (DMZ), are more exposed for hacking. All remote access should to be secured over Virtual Private Network (VPN) with a two-element verification framework set up and in addition to this for more security in basic frameworks; two-element confirmation should be set up over all frameworks.

3.5. Physical vulnerabilities:
Physical vulnerabilities can be referred to as physical setup like bad substations, wind ranches, or server rooms all posture potential danger to a framework. If these are a piece of a protected or basic system then they should be vigorously secured. Access control with bookkeeping is important at these physical areas. There should be more security protocols for gadgets. Switch security can be utilized on systems to prevent potential assailants from putting in their own Ethernet link (by locking interchanges
to the first MAC address as it were). USB ports on PCs and Servers should be debilitated by equipment so that malware would be extremely hard to be installed physically. [9] General outline of the attack can be defined using simple flowchart which includes various phases.

![Diagram](image)

**Figure 1.** General Outline of the attack.

The various types of attacks are:

3.6. **Eavesdropping:**
Eavesdropping or spying is a serious issue and is considered as passive attack including the assailant latent listening to the data passed on by a smart meter or a smart metering passage to the administration suppliers. Such attack influences the protection of client and can be effectively performed over a remote correspondence channel or an electrical cable. The discovery of such attack is exceptionally troublesome. Such an attack can generally be dispatched through the WAN and by an inquisitive neighbor or a thief for different reasons.

3.7. **Denial of Service Attacks:**
Denial of Service attack focuses in general, smart metering foundation, the smart grid or part of the network. Such attack can be performed, for instance by an enemy by sending numerous more charges than anticipated to the smart metering gateways or on the flip side to the utility servers. This will make the framework at risk level which might not be ready to react to the authentic solicitations. It will basically close the matrix or piece of framework for vital administrations. The extent of this attack is the entire matrix or parts of a network. Such attacks can be dispatched through the WAN.

3.8. **Packet Injection Attacks:**
Packet Injection attack can be dispatched by infusing false packets e.g., false commands for a smart meter, into the system. This may be done to slice power, to parts of the smart metering framework. This attack can also be used to trade off the charging process by creating false bills costing the clients and utilities a considerable measure of cash. Such attacks will regularly be propelled from the WAN.

3.9. **Malware Injection Attacks:**
Malware Injection attack is mainly caused by infusing malware into the system which can propel this attack. This will influence the correspondence between gadgets in the matrix and bargain the charging and reporting forms. The interest/utilization status of the grid is disturbed in order to destabilize the heap on the matrix. The extent of this attack can possibly be up to the entire smart metering framework. Such attacks can be propelled from the WAN.

3.10. **Man-in-the-center Attacks:**
A man-in-the-center attack is a sort of attack in which an attacker "embeds" himself between communicating clients. An attacker makes an association with both the clients, catches their messages
and transfers them to the next end and makes each of them believe that they are talking specifically to each other. In this manner, the attacker has the opportunity of either inactively listening stealthily or adjusting the data being traded between the clients.

B Min [10] discusses further Malware attacks targeting cyber physical systems and proposes these types of attacks as the attacks which remain undetected as their impact is physical. This type of attack can be considered as deceptive attack as the attackers ensure that the operators do not notice their activity and whether system is under attack. Genuine malware attacks effectively infect and modifies several CPS and makes them malfunction. It also dishonestly reports general data and prevents it from recovering. Three basic requirements for deceptive attack: Modifying the behavior of target physical devices, hiding physical impact via software or data manipulation, preventing automatic and manual recovery attempt. These attacks are multistage attacks since most of CPS attacks include power plants and other smart grid subsystems and are set up using customized commercial off the shelf COTS hardware and software solutions.

B. Min [10] also discusses a very important attack which is a combination of characteristics of smart grid and above discussed CPS related malware attacks.

3.11. Smart Grid Blackout Attack:
This focusses on both nullification of built in security structures like self-healing and validation in smart grid and CPS related malware attacks. There are several phases during attack. First phase is initialization phase. In this target subsystems are attacked by penetrating wide range of attack vectors. After this the system installs cyber espionage malware on attacked targeted subsystems and starts gathering data on the systems and configures the smart grid systems and networks. As the architecture of smart grid is huge and complex it’s not easy to get total control over the system, for that reason it targets small systems one by one and penetrates from one system to other. During propagation from one system to other malware can self-replicate to other systems on LAN to find target network systems and field devices. This process continues until the attack finds target field devices to modify at the phase of deceptive attack. Next phase involves gathering of information and organization. In this phase already installed malware carries out cyber surveillance tasks and collects required information from SCADA systems. The malware uses HTTP and RPC with encrypted protocol which makes security systems to detect it. Also collected data stored in the infected system is encrypted to make it difficult for analysis. [10]

4. The main Solutions and Architectures

4.1. Encrypted Communication:
The main goal of Encrypted Communication technique is to see that correspondence between the elements in the smart metering frameworks is encrypted. The encrypted correspondence is regularly accomplished by utilizing existing conventions, for example, TLS. TLS is not viewed as secure any longer and in this way different methodologies must be consolidated with TLS to make encryption stronger. These incorporate application layer encryption notwithstanding TLS to fortify the general encrypted correspondence. An illustration is the insurance profile (PP) based methodology created in Germany by the BSI, otherwise called the BSI PP. They propose double encryption, at the application layer to guarantee end-to-end encryption and at the vehicle layer.

4.2. The Privacy-saving Authentication Scheme for a Smart Grid Networks (PASS):
The Privacy-saving Authentication Scheme for a Smart Grid Networks (PASS) includes the utilization of smart apparatus (situated at clients' homes) connected with an alter safe gadget for producing pseudo personalities and marks on messages. A client is given this gadget when he/she opens a record or registers a recently obtained smart machine. B.Min, V.Varadharajan [10] describes how the attacks can be detected and blocked by applying suitable defensive techniques.

4.3. Gateway based Approach:
Gateway is a latest way to deal with smart metering, proposed by European nations, like Germany and the UK. A gateway is an empowering innovation for future communications between the smart meters and the smart grid. A gateway (or smart metering gateway) goes about as a correspondence unit between the metering gadgets in the client premises and the utility. The portal not just serves as a correspondence and control unit between the meters and the utility, but on the other hand is responsible for the guarantee of the protection of client. One passage oversees the smart meters and other smart gadgets introduced in a house or a premise. The gateway intermittently speaks with the utility servers by means of WAN.

4.4. Interruption Detection Systems:
Interruption Detection Systems (IDS) and Intrusion Prevention Systems (IPS) could be utilized as a part of the systems of a smart metering framework. This gives recognizable proof of interruptions, location of rebel hubs or wellspring of attacks and rejection of these hubs from further correspondence in the system. F.Siddiqui, S.Zeadally, C. Alcaraz, S.Galvao [11] further proposes some more architecture for smart grid Privacy.

4.5. Blind signature:
Blind signature consists of following procedures:
First party signs a message created by second party with no knowledge of its original data. Third party receives the signed message. It verifies that the message is authorized by first party. The consumers prepare a set of credentials, each stating the amount of electricity requested. Customer requests the control center to sign them unseeingly so that they can submit any of these credentials to request of electricity. In this process Client 1 is unaware of the valid data sent by Client 2, this data is verified using a protocol which is used in e-cash system. Client 2 generates ‘a ‘data using various blinding platforms. It then blinds the ‘a’ data and transmits it to Client 1. Client 1 randomly selects ‘b’ data (b<a) and asks Client 2 to reveal the b blinding factor. If ‘b’ blinding factors are valid, Client 1 accepts the request for authentication and verifies the remaining (b-a) data. When a consumer presents a credential secretly, the control center cannot verify which customer is making the request but can verify the signature to confirm that it has been received from valid consumer. [11]

4.6. The 3rd Party Escrow Architecture
The 3rd Party Escrow Architecture helps in anonymizing high frequency energy measurement data using pseudonymous identity (ID)
- It has two separate IDs
- Two Ids are High Frequency IDs (HFID) and one Low Frequency Id (LFID)
- HFIDs are anonymous
LFID can be assigned to a consumer or smart meter. The confidentiality is implemented by keeping HFID secret to the utility or the smart meter installer. The HFID is ‘secret’ inside the smart meter, or hard-coded to be used for all HFID related messages. For the utility to authenticate the legality of the HFID, a 3rd party Escrow mechanism is implemented. The 3rd party can build smart meter itself or can outsource the work to a valid third party. This third party will also have an authentication to access this information. The manufacturer can assign two unique IDs to each smart meter that is produced, only one of which (LFID) is visible to the utility, both during the procurement and distribution procedures. [11]

5. Conclusion
Cyber security and privacy issues in the smart grid are new areas in the fields of power industry and electrical engineering. Increased interconnection and integration introduces cyber vulnerabilities into this grid and should be provisioned in smart grid designs. This requires different designs of traffic routing to meet the required privacy properties. Current reviewed schemes of accountability don’t address all the above issues. Thus, in conclusion any communication paradigm used in a smart grid should support all aspects of privacy such as ambiguity, uncertainty, indistinct, unmanageability and undetectably. In the coming years, the trend in energy management system of the home of intelligent home will become increasingly apparent. Application and development of Bluetooth and ZigBee are most appreciated by the industry in the recent years. Of the two types of technology, ZigBee supports low cost and more knots, and with its low power consumption, is set to become an important part of communication technology for the intelligent home. Because the ZigBee specification SEP2.0 support multiple functions of the network technology, a product can be compatible with a variety of communication methods to connect to the home network and home automation. [12].

References
[1] “Security Issues in Smart Metering Systems “Obaid Ur-Rehman, Natasa Zivic, Christoph Ruland
[2] “Cyber Security and Privacy Issues in Smart Grids” J Liung, Y. Xiao, S Lui, C.L Phillip Chen.
[3] R. Kailar, “Accountability in electronic commerce protocols,” IEEE Trans. Softw, Eng., vol. 22, no. 5, pp. 313–328, May 1996.
[4] M. Kudo, “Electronic submission protocol based on temporal accountability,” in Proc. 14th Annu. Comput. Secur. Appl. Conf., 1998, pp. 353–363
[5] “Accountability in Smart Grids” Jing Liu, Yang Xiao, Jingcheng Gao.
[6] Hastings, John, David M. Laverty, and D. John Morrow “Securing the smart grid”, 2014 49th International Universities Power Engineering Conference (UPEC), 2014.
[7] M. Stegelmann and D. Kesdogan, ”GridPriv: A Smart metering architecture offering k-anonymity,” in Proc. IEEE 11th Int. Conf. Trust, Security Privacy Comput. Commun., Jun. 2012, pp. 419-426.
[8] X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, “ASRPAKE: An anonymous secure routing protocol with authenticated key exchange for wireless Ad Hoc networks,” in Proc. IEEE ICC, Jun. 2007, pp. 1247-1253.
[9] Hastings, John, David M. Laverty, and D. John Morrow, ”Securing the smart grid”, 2014 49th International Universities Power Engineering Conference (UPEC), 2014.
[10] “Design and Analysis of Security Attacks against Critical Smart Grid Infrastructures “B. Min, V. Varadharajan.
[11] “Smart Grid Privacy: Issues and Solutions” F. Siddiqui, S. Zeadally, C. Alcaraz, S. Galvao.
[12] “Application and Development of ZigBee Technology for Smart Grid Environment” Sheng-Fa Chang1, Chi-Feng Chen1, Jyh-Horng Wen1, Jih-Hsin Liu1, Jun-Hong Weng1, Jian-Li Dong2.