Int. J. Communications, Network and System Sciences, 2014, 7, 151-163
Published Online May 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.75017

Scientific Research

Sensing the Nation: Smart Grid's Risks and Vulnerabilities*

Adedoyin Olayinka Ajayi[1], Boniface Kayode Alese[1], Sunday Emmanuel Fadugba[2], Kolade Owoeye[2]

[1]Department of Computer Science, Federal University of Technology, Akure, Nigeria
[2]Department of Mathematical Sciences, Ekiti State University, Ado Ekiti, Nigeria
Email: dedoyyin@gmail.com, kaalfad@yahoo.com, emmasfad2006@yahoo.com, kolade_owoeye@yahoo.com

Received 7 April 2014; revised 2 May 2014; accepted 12 May 2014

Abstract

This paper presents issues and trepidations associated with transferring from conventional methods of electricity monitoring and distribution to the cyberspace, especially in developing countries like Nigeria where current approaches have failed to provide regular, reliable electric power. The Smart Power Grid is a developing concept already put to test, successfully, in very advanced countries. The implementation of the Smart Grid will include the deployment of many new technologies and multiple communication infrastructures. Connecting the electricity grid to the Internet can provide a lot of advantages in terms of control, data viewing and generation. However, in Nigeria, the proposal to transfer conventional methods to the Smart Grid has perhaps not hit the deck yet because of excessive focus on power generation, and because of the annotated reservations associated with the Internet, as the Smart Grid involves circulation and dispersal via inter-networking structures. This paper describes the key technologies that support Power Grid substation automation, summarizes the mode of implementation into the existing Nigerian electrical infrastructure and brings fore issues and mitigating approaches to provide a seamless and securitised transfer of the current power grid to the Smart Grid.

Keywords

Power Grid, Conventional Methods, Cyberspace, Smart Grid, Developing Countries

1. Introduction

The supply of stable and sustainable electricity to consumers has been described as the backbone of socioeconomic development of any nation [1]. The power sector of the Nigerian economy has been chaotic as with other

*Risks, vulnerabilities and solutions involved in migrating from conventional practices to a Smart Grid.

How to cite this paper: Ajayi, A.O., Alese, B.K., Fadugba, S.E. and Owoeye, K. (2014) Sensing the Nation: Smart Grid's Risks and Vulnerabilities. *Int. J. Communications, Network and System Sciences*, **7**, 151-163.
http://dx.doi.org/10.4236/ijcns.2014.75017

sectors of the economy. The focus has too many times been on power generation rather than a balanced emphasis on generation, circulation and monitoring. There are three major dams generating the country's electrical needs—the Kanji Dam, the Shiroro Dam and the Jebba Dam. The Kanji Dam, for instance, was designed to have a generating capacity of 960 Megawatts (MW); however, only 8 of its 12 turbines have been installed, reducing the capacity to 760 MW and, in recent years, a reduced capacity of not more than 450 MW is due to poor maintenance, as it has not been overhauled since its establishment [2] [3]. The poor electricity platform provided to the citizenry, industry and other vital aspects of the societal economy has had a backlash, catapult-like effect on other issues such as climate change [4], unemployment [5], and ridiculously extreme rates of telecommunication infrastructures. The problem of the Nigerian electrical grid is not purely administrative as several billions of Naira has been lost to vandalism to power equipment for both high and low tension purposes [6]. The nation's government continues to fuse about increase in power generation when it has become imperative to promote efforts in efficient methods of power distribution and monitoring.

The Smart Grid, in its simplest definition, means adding computer and communications technology to the existing utility grid [7]. It refers to an improved utility supply chain that runs from a major plant all the way inside a home. Smart grids could be deployed over utility systems like electricity, water supply and crude oil structures. In the context of this research, Smart grids are modern electricity networks that deliver energy to end users via automated digital technology; *i.e.* the application of modern information, communication, and electronics technology to the electricity delivery infrastructure as shown in **Figure 1**. They are energy-efficient, thus reducing cost by billions and increasing reliability and transparency. They increase the cooperation and connectivity between various sources and suppliers of energy from hydro-power to thermal, or nuclear to coal. Nigeria generates electricity primarily through hydro power and oil, but plans to use coal and liquefied natural gas. It could also employ solar, wind and possibly, thermal energy, and if it revived its now defunct nuclear power program, it could take advantage of that as well for energy purposes [8]. Smart grids are the energy picture of the future (see **Figure 2**) and various nations and municipalities have staked their claim on them.

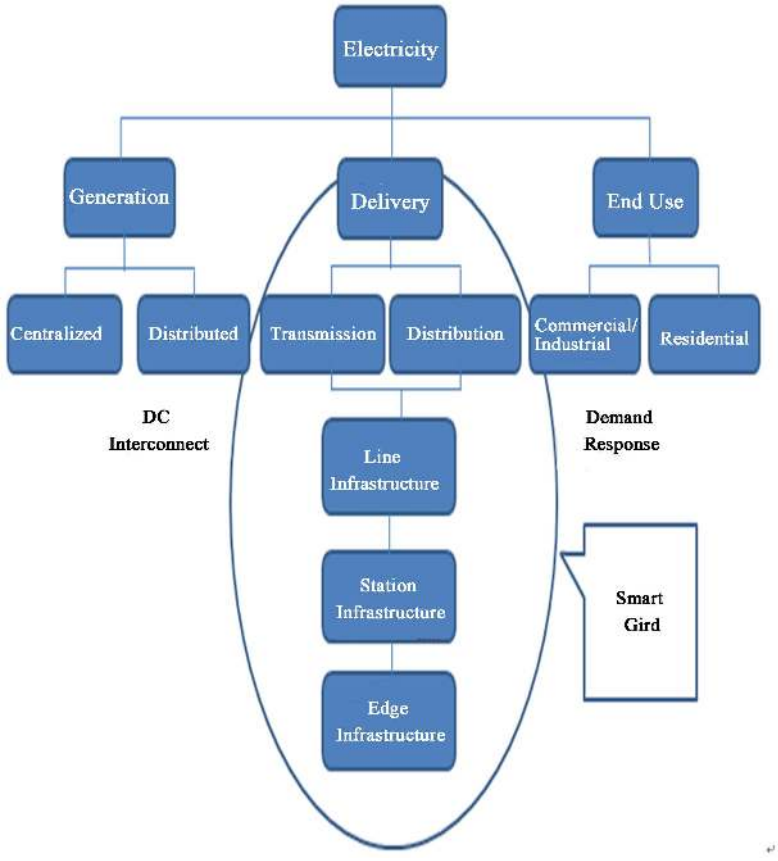


Figure 1. The Smart Grid.

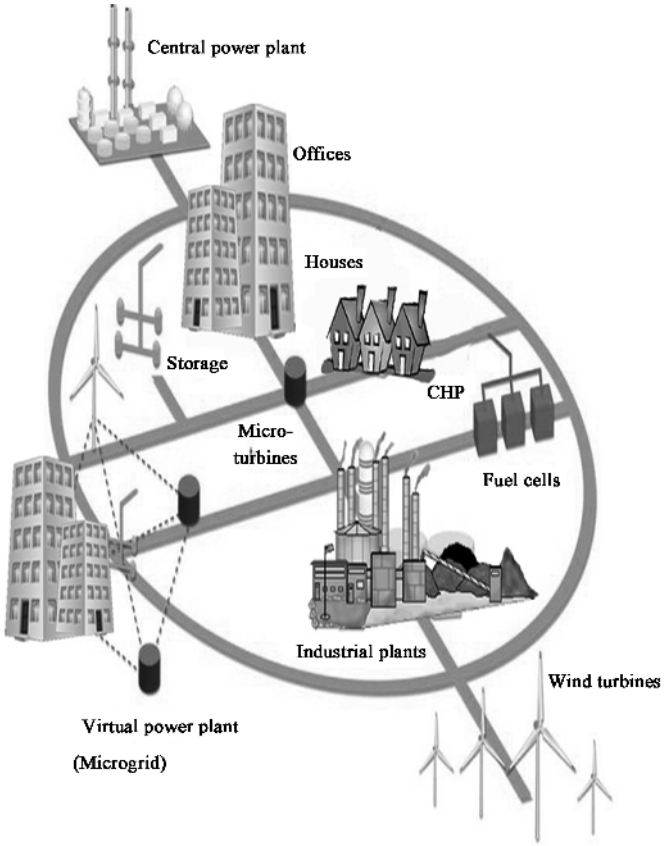


Figure 2. The vision of the Smart Grid. Source [9].

The US Department of Energy [8] [9] specified the benefits of smart grids as follows

1) Smart grids detect problems and automatically solve them (self-healing),
2) Consumers can participate in the functions of the grid, changing their behaviour if it needs. Customers can easily access usage and other information (visibility),
3) Smart grids resist security attacks,
4) Smart grids accommodate all generation and storage options,
5) Encourages innovation is highly efficient,
6) A Smart Grid can optimize capital assets while minimizing operations and maintenance costs,
7) Creating an electricity market as significant increases in bulk transmission capacity will require improvements in transmission grid management. Such improvements are aimed at creating an open marketplace where alternative energy sources from geographically distant locations can easily be sold to customers wherever they are located.

A Smart Grid has integrated in an intelligent monitoring system that keeps track of all electricity flow in the general system. The Smart Grid also makes sure of less power loss by incorporating super-conductive transmission lines, as well as the aptitude of integration of alternative power generation sources such as solar, wind and liquefied natural gas. When power is least expensive, a Smart Grid could turn on selected home appliances such as laundry apparatuses or industrial processes that can run at capricious hours [7]. At peak times, it could turn off certain utilities to condense demand. In more technical terms, the Smart Grid is a simple upgrade of conventional power grids, which transmit electricity from limited central power substations to a large number of consumers, to one that has a sustained capability to rout power in more optimal methods in riposte to a very wide range of conditions including those that are environmental (weather change causing little or no rainfall for hydro-power generation for instance), commercial (e.g. first-class price rates for consumers that use power at peak times), local (for instance, on the grid itself, like transformer failures) or in the home (e.g. someone leaving for work shutting all appliances off) which could affect the rates of flow of electricity.

2. How the Smart Grid Works

2.1. The Smart Grid Network

The Smart Grid has installed within it a fully operational two-way communications network between electricity suppliers and its consumers. The communications channel will support modern energy concepts such as concurrent or real-time estimation of price, consumption supervision, load shedding, energy saving, rate reduction as a result of low peak discount, cost savings from energy efficiency, integration of plug-in hybrid electric vehicles (in advanced countries only), and the incorporation of distributed energy generators such as wind turbines and photovoltaic systems. This new network will be constructed using various communication paths including fiber optic cable, hybrid fiber coax, twisted pair, broadband over power line, and wireless technology [10].

Figure 3 shows network connections that can be traced from the customer's premises to collector nodes to the utility control centre and to transmission and distribution substations where electronic controllers are located that control the generation and flow of electrical power. The residence block in **Figure 3** represents the Home Area Network (HAN) that may include communicating Smart Grid components such as a Smart Thermostat, Smart Water Heater, Smart Appliances, and Plug-in Hybrid Electric Vehicle (PHEV)/storage. All the HAN devices are connected to a Smart Meter through a network such as Zigbee or mesh wireless [10]. The Smart Meter connects the HAN to a collector node also through a network such as Zigbee or mesh wireless and may also communicate with the HAN networks located nearby. Collector nodes communicate with the utility through common communication mechanisms including the Internet. Intranet communication paths within the utility area include an Access Control scheme that is designed to impede the flow of unauthorized messages.

2.2. Smart Grid Technologies

As with the whole concept of the Smart Gird, future utility companies hope to deliver energy and information to customers through a "smart" energy supply chain created by the convergence of electric, communication and information technologies that are highly automated for responding to the changing environment, electricity demands and customer needs. Composed of many independent systems, the Smart Grid will evolve by integrating existing islands of automation to achieve value through the delivery of information to customers, grid operators, utility companies and other stakeholders. A reliable and secure Smart Grid holds the promise of enabling auto

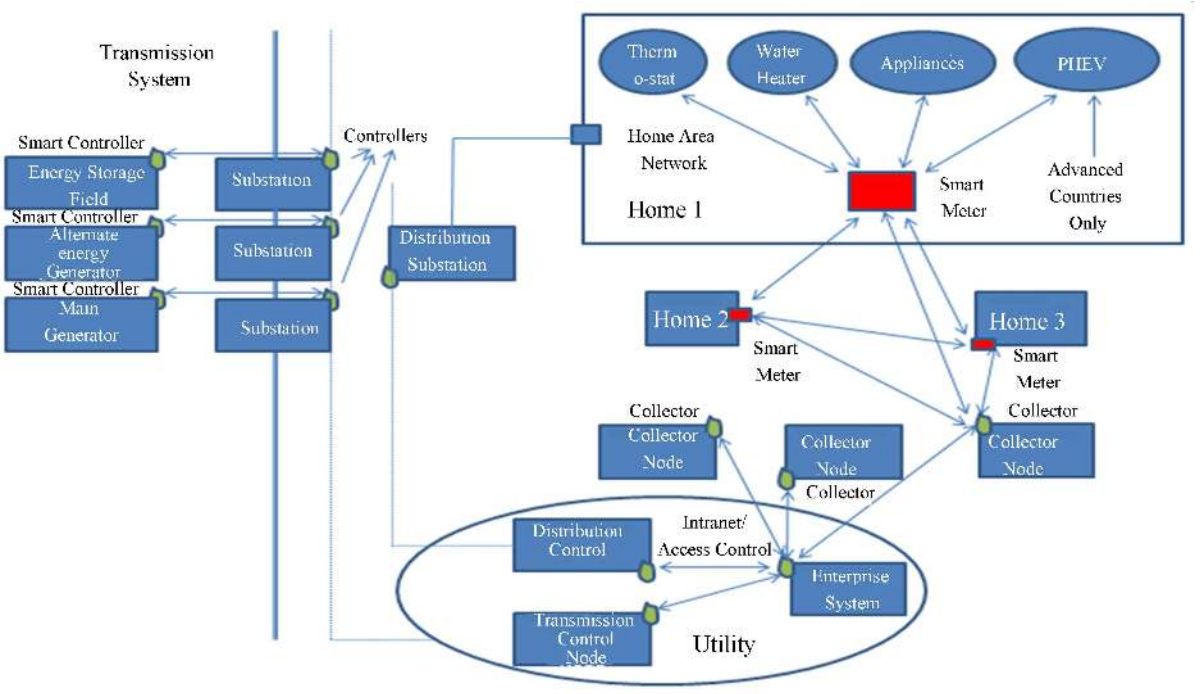


Figure 3. Typical Smart Grid components and connections.

mated demand response, providing customers a myriad of options to manage their energy costs through technology enabled programs along with limiting outages with a self-healing resilient transmission and distribution network and other strategically important functions. The building blocks of this Smart Grid include AMI, advanced transmission and distribution automation, distributed generation, electric vehicle refuelling infrastructure and renewable energy generation projects of today [11]. The emergence of this new class of Smart Grid systems holds tremendous promise and requires innovation and deployment of new technologies, processes and policies. As mentioned above, the implementation of the Smart Grid will include the deployment of many new technologies including advanced wireless sensors to improve situational awareness, advanced metering, automatic meter reading, and, as mentioned earlier, integration of distributed generation resources such as photovoltaic arrays and wind turbines. These new technologies will require the addition of multiple communication mechanisms and communication infrastructures that must be coordinated with conventional systems and technologies. An important component of the Smart Grid is the Supervisory Control and Data Acquisition (SCADA) component. SCADA is a concept that is used to refer to the management and procurement of data that can be used in developing process management criteria [9]. Infrastructures like electricity which is controlled by SCADA can play a huge role on Smart Grids. According to [9], the use of the term SCADA varies, depending on location. In North America, SCADA refers to a distributed measurement and management system that operates on a large-scale basis. For the rest of the world, SCADA refers to a system that performs the same basic functions, but operates in a number of different environments as well as a multiplicity of scales. SCADA systems are primarily control systems. A typical control system consists of one or more Remote Terminal Units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station. For the most part, the brains of a SCADA system are performed by the Remote Terminal Units (sometimes referred to as the RTU). The Remote Terminal Units consists of a programmable logic converter. The RTU are usually set to specific requirements, however, most RTU allow human intervention, for instance, in a factory setting, the RTU might control the setting of a conveyer belt, and the speed can be changed or overridden at any time by human intervention. In addition, any changes or errors are usually automatically logged for and/or displayed. Most often, a SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention.

One of key processes of SCADA is the ability to monitor an entire system in real time. This is facilitated by data acquisitions including meter reading, checking statuses of sensors, etc. that are communicated at regular intervals depending on the system. Besides the data being used by the RTU, it is also displayed to a human that is able to interface with the system to override settings or make changes when necessary [9]. SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre-programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system. The goal of human-machine interaction engineering is to produce a user interface which makes it easy, efficient, and enjoyable to operate a machine in the way which produces the desired result. This generally means that the operator needs to provide minimal input to achieve the desired output, and also that the machine minimizes undesired outputs to the human. Ever since the increased use of personal computers and the relative decline in societal awareness of heavy machinery, the term user interface has taken on overtones of the (graphical) user interface, while industrial control panel and machinery control design discussions more commonly refer to human-machine interfaces.

Aside from SCADA systems, there are structures in place for energy administration. Energy-Management Systems (EMSs) are a typical example, while we also have Distributed Control Systems (DCSs). **Figure 4** illustrates conceptually the strongest relationships between the various infrastructure requirements and the various Smart Grid capabilities as captured in [12].

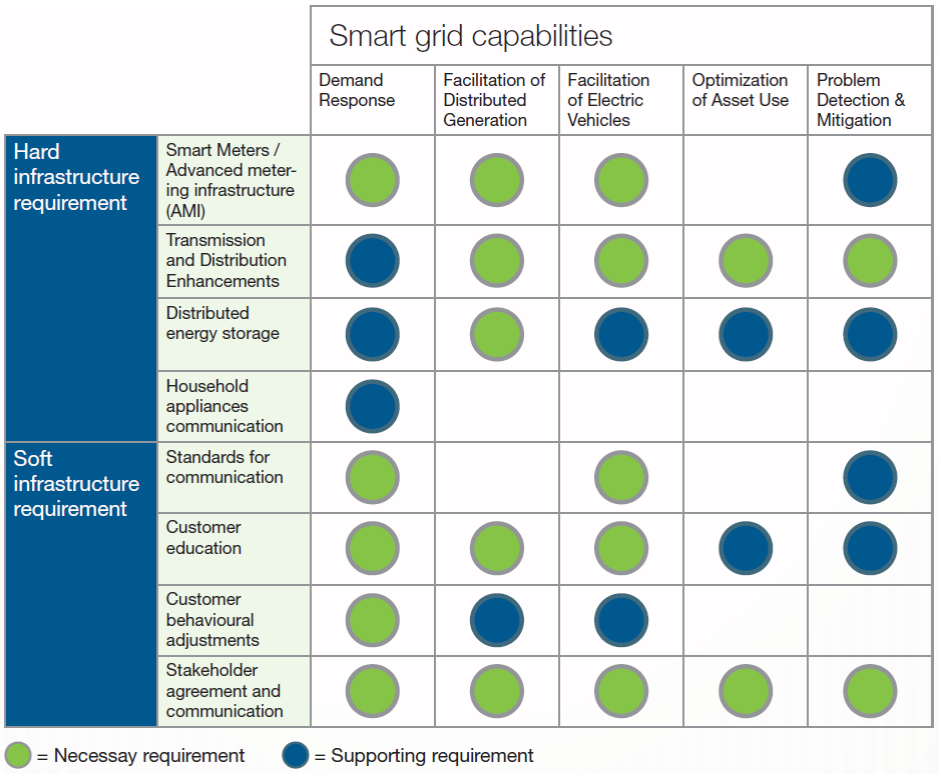


Figure 4. Relationship between infrastructure and various smart grid capabilities (source [12]).

3. Security Issues and Analysis of Challenges in Smart Grid Technologies

The Smart Grid system is a networked and integrated infrastructure. The Smart Grid's electricity transmission and distribution facilities also rely on data communications to optimize the transmission and distribution process. The Smart Grid vision and its increased reliance on IT systems and networks expose the electric grid to potential and known cybersecurity vulnerabilities associated with using such systems.

1) Vulnerability to Sabotage

The Smart Grid means more information technology, and some observers worry that it will be vulnerable to sabotage. A CNN article in 2009 [13] cited tests showing that "a hacker can break into the system", and cybersecurity experts have demonstrated that certain smart meters can be successfully attacked, and the impact of such attacks includes the ability to disrupt the electricity grid [12] [13].

Further, a hacker, with only $500 (about N80,000) in equipment and a limited electronics and engineering background could "take command and control of the advanced meter infrastructure (AMI) allowing for the en masse manipulation of service to homes and businesses". [12] [14] pointed to two steps that could mitigate these security risks: first is an industry standard; second, "an open platform, which will allow developers to be able to contribute their best solutions".

2) Invasions of Privacy

A number of Smart Grid experts believe the risk of potential privacy violations has not received adequate attention. As [15] noted, the Smart Grid "introduces the possibility of collecting detailed information on individual energy consumption use and patterns within the most private of places—our homes". Great care must be taken to prevent a sacrifice of consumer privacy. Information proliferation, lax controls and insufficient oversight of this information could lead to unprecedented invasions of consumer privacy.

3) Increase in Attack Paths

Increasing the use of systems and networks increases the number of entry points and paths that can be exploited by potential adversaries and other unauthorized users [16]. Also, increasing the use of new system and network technologies can introduce new, unknown vulnerabilities. The electricity industries in advanced nations do not have metrics for evaluating cybersecurity. The utilities' focus is on regulatory compliance instead of

comprehensive security. There is a lack of security features being built into Smart Grid systems. The electricity industry lacks an effective mechanism to disclose information about Smart Grid cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices in the industry.

Smart Grid security risks and vulnerabilities can be identified by using a top-down or bottom-up approach [17]. The top-down approach, according to [17], analyses well-defined user scenarios such as Automated Meter Reading (AMR) billing, while bottom-up approach focuses on well-understood security attributes and features such as integrity, authentication, authorization, key management and intrusion detection. One of the strongest arguments made for securing smart meters is that consumers will have physical [18], and potentially logical access to the smart meters. Security is generally described in terms of availability, integrity, and confidentiality. Cyber systems are vulnerable to worms, viruses, denial-of-service attacks, malware, phishing, and user errors that compromise integrity and availability [19].

Different literatures, like [20]-[22], also carried out research on the classification of Smart Grid risks, vulnerabilities and security attributes. The most widely discussed security challenges in these literatures concern the protection of smart metering data and the Supervisory Control and Data Acquisition (SCADA) field devices in the Smart Grid against unauthorized access and repudiation. This is an important part requirement without which AMR data, for instance, will not be trusted by either the utility provider(s) or the customers.

The widely accepted elements (aims, principles, qualities, characteristics, and attributes) of information security are stated in [23] and [24] as follows—confidentiality, integrity, availability, authentication, non-repudiation and access control. The first, fourth and last elements mentioned above are perhaps most important; one of the important security tasks is to assure efficient security access control (SAC), e.g. to differentiate between "proper" access of "fit" individuals (persons to which access was intended only) and all other attempts of access [25], ensuring that an authenticated user accesses only what they are authorized to and no more [26] [27]. In a Smart Grid, security is required in different levels; end to end secure communication protocols need to be used, hardware components (e.g. the smart meter) need to withstand physical attacks, the grid needs to detect forged/hacked components, and also detect intrusive activities, smart meter software should be bug-free etc. [28]. It is also equally important to develop mechanisms for protecting smart metering data against insider attacks and for protecting field devices against intrusion attacks. This is to make sure that users access smart metering data and data from field devices in an authorized manner and will only use this data in an "acceptable" manner. [22] addresses some of the problems of local intrusion detection for field devices in the Smart Grid. Smart grids have unintended consequences for customer privacy. The use of the smart meter is central to this effect. Energy user information stored at the meter and distributed thereafter acts as an information-rich side channel, exposing customer habits and behaviours. Certain activities, such as watching television, have detectable power consumption signatures. History and literature has shown that where financial or political incentives align, the techniques for mining behavioural data will quickly evolve to match the desires of those who would exploit that information [28]. Thus moving to a smart electrical grid in a country like Nigeria is imperative not only for the nation but also for the planet. However, we must be realistic about the risks and anticipate and mitigate the security and privacy problems they introduce, because in moving to the Smart Grid, we replace a physical infrastructure with a digital one. When securing the Smart Grid, one of the biggest challenges is prevent hackers from wreaking havoc, like turning power off to customers, perhaps cities at will. In 2008, the United States Central Intelligence Unit confirmed that criminals had hacked into computer systems via the Internet and cut power to several cities [29]. Cybercriminals looking to profit from attacking the Smart Grid, seek to breach power distribution software and databases.

Spoofing and phishing (when a system or program masquerades as another) are fraudulent activities used to gain access to confidential information on a network [30]. In 2008, Intel developed hardware solutions to help combat the issues of spoofing and phishing. It provided encryption methods and stores for critical security codes and the assurance that they are only decrypted at the executing environment that originally encrypts them. Intel also developed ways to prevent the booting of a compromised system where the control, possibly infected by a virus or connected to an illegal peripheral need to be deactivated to prevent damage. It achieved this by creating an initial trusted state and comparing the hash (a number generated by a formula of all system software of the trusted state) with the current state, while blocking system start up attempts when differences are detected [30].

[9] summarized the various functions a grid must have. Smart Grid must have the following functions: self-healing, consumer participation, resist attack, high quality power, accommodate generation options, enable electricity market, optimize assets, enable high penetration of intermittent generation sources.

3.1. Grid Information Security Functional Requirements

[31] introduced the concept of hermeneutic circle and information security functional requirement identification. As already affirmed, information security for the grid market cover smatters including automation and communications industry that affects the operation of electric power systems and the functioning of the utilities that manage them and its awareness of this information infrastructure has become critical to the reliability of the power system. According to [31], focusing on the grid information security functional requirement is a step ahead in developing consumer trust and satisfaction toward Smart Grid security completeness. They identified the functional requirements and related their significance addresses to the consumer requirements of information security of a Smart Grid. Vulnerabilities may bring forth possibility for an attacker to penetrate a network, make headway admission to control software, alter it to load conditions that destabilize the grid in unpredictable ways. In the process of identifying information security functional requirement, the significant relationship to consumer requirement is taken into consideration as how it would impact consumer trust and satisfaction [31]. It refers to the consumer requirements developed [32].

Some of the consumer requirements discussed in [31] include confidentiality, integrity, availability, cryptography and key management, reliable systems level, networking issues, tactical oversight system, privacy concerns, high bandwidth of communication channels, proprietary protocols and facilities misuse prevention. Functional requirements were discussed with the reference to the consumer requirements identified, respectively:

1) Information access control: as mentioned in [27], in an open system, all form of information should be secured by protocols against unauthorized access, or alteration, disclosure or destruction and against accidental loss or destruction, and thereby eliminating access to customer property.
2) Authenticity: as aforementioned in [23], security is a consolidative concept that covers notions of availability, authenticity, confidentiality, integrity and non-repudiation. To ensure unconventional information modification, loss or destruction, non-repudiation and authenticity must be ensured [33]. Also, to ensure that data is not exploited, integrity and authenticity is mandatory.
3) Data and backup recovery: the system must be dynamic and scalable, always managing, deploying and furbishing up a technology or solution target to maximize the benefits of systems and technology which facilitate to control IT risk [34]. Procedures were developed aiming to render restoration, backup, offsite storage and disaster recovery consistent with the entity's defined system availability and associated security policies [35].
4) Trusted network: vulnerabilities in the system can open such system to (outsider or insider) attacks and bring forth possibility for such attackers to penetrate the network, and gain unauthorized access to system control software. This kind of unauthorized access can lead to the attacker making alterations to load ill-defined or external conditions to destabilize the grid in unpredictable ways. Therefore, approaches to secure networked technologies and to protect privacy must be designed and implemented, in a forward-thinking approach, in the transition to the Smart Grid.
5) Interoperability and security: interoperability here is closely related to the scalability concept describe above in 3). The interoperability proffered by IP has enabled converged networks that provide both data and voice to become common in businesses [36], and a variety of triple play providers currently offer residential data, voice, and video on converged networks [37]. Interoperability is a primary or essential component of borderless Smart Grid networks, and its cyber security platform must be secured.
6) Cyber security guidelines: in developed nations, federal government agencies have developed, or are currently developing more security guidelines and best practices for Smart Grid [38]. As cyber-technology has provided more grounds and instruments to be used b terrorist organizations, the notion of cyber terrorists has been created. Cyber terrorists attack technological features such as the Internet in order to help foster their cause [18]. The utilization of Internet and related IP and wireless technologies exposes the system to easy, remote, external cyber threats. The notion of cyber threats, often referred to as cyber warfare [39] is one used to describe informationalised wars. These threats often include attacks on public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are dependent on computers for daily operations. Hence, the nature of the responses in term of necessary to preserve the future security of our society become prior to action.
7) Law enforcement: when the public sharing of information about a specific location's energy used is possible, law enforcement plays a significant role, particularly when the concern exists that the prevalence of raw energy data could lead to actions on the part of criminals who will look to exploit the public contents and thus

incur a reaction from law enforcement agents/agencies.

8) Improved wireless technology: wireless networks are commonly used in the current Smart Grid deployments [10]. According to NSTB, wireless networks were employed because they have some significant advantages over other alternatives. Wireless devices are plentiful and inexpensive. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and a larger range. However, mesh networks are vulnerable to attack by an intelligent adversary. Because most wireless communication standards such as ISA 100.11a are in the early stages of development and deployment, there is not much publicly available information regarding their security [10]. This implies a need for more security research on IEEE 802.15.4-based networks and other wireless networks intended for AMI. It has therefore become necessary to provide means to combat intrusion, and other denial of service attacks, in wireless network devices deployed in the Smart Grid.
9) Cryptographic protocols & encryption policies: cryptographic algorithms are necessitated to convert plaintext into cipher text and vice versa [23] [40]. The conversion of plaintext into ciphertext makes it impossible for an attacker to possess plaintext from a ciphertext without a recognized key. It is a sequence of bits and serves as a parameter for transformation. In an area aiming to provide secure authentication and communication services in online notification systems, cryptography techniques are highly beneficial. Moreover, It is relatively well known that the encryption policies such as encrypting sensitive data that is either at rest in databases or in motion such as portable devices, emails and instant messages [31] [41] can help to minimize the probability of insider misuse. Technical control insider attacks are being negated through encryption techniques against [31] [42].

3.2. Future Research Directions

The matching of consumer requirements and functional requirements of information security of the Smart Grid provides an interesting prospect for future research development. But of particular emphasis is the concatenation of last two items on list of functional requirements—improved wireless technology, and cryptographic protocols & encryption policies. Current researches have introduced the concept of Wireless Sensor Networks (WSN). Wireless Sensor Networks (WSN) consist of small devices—called sensor nodes—with radio, processor, memory, battery and sensor hardware. Researchers have documented some common challenges associated with wireless sensor networks. Some of them include: probabilistic channel behaviour, accidental and directed interference or jamming, and eavesdropping or unauthorized modification of the communications if not protected by authentication and encryption. Also, the distributed nature of WSNs makes energy-efficient protocol design particularly challenging, as there are unique problems in self-configuration, network discovery, medium access control and multi-hop routing. Further, attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Major attacks in WSN are DoS, attacks on information in transit [43], sybril attack [44], blackhole attack [45], hello flood attack [46] and the wormhole attack [47], all labelled insider attacks. In an outsider attack, the attacker node is not an authorized participant of the sensor network. Encryption techniques and also authentication schemes prevent such an attacker to gain any special access to the sensor network. The intruder node can only be used to launch passive attacks, like passive eavesdropping (the attacker eavesdrops and records encrypted messages, the messages may then be analysed in order to discover secret keys), denial of service attacks (an adversary attempts to disrupt the network's operation by broadcasting high-energy signals; in this way, communication between legitimate nodes could be jammed, or even worse, nodes can be energy depleted) and replay attacks (the attacker captures messages exchanged between legitimate nodes and replays them in order to change the aggregation results). Thus, security mechanisms such as encryption and authentication are essential to protect information transfers. However, existing network security mechanisms are not feasible in this domain, given the limited processing power, storage, bandwidth and energy resources. Public-key algorithms, such as RSA are undesirable, as they are computationally expensive. Instead, symmetric encryption/decryption algorithms and hashing functions are between two to four orders of magnitude faster, and constitute the basic tools for securing sensor networks communications. Recently, Elliptic Curve Cryptography (ECC) has emerged as an able alternative to RSA-based algorithms, as the typical size of ECC keys is much shorter for the same level of security. Even though elliptic curve cryptography is feasible on sensor nodes, its energy requirements are still orders of magnitude higher compared to that of symmetric cryptosystems.

Therefore, elliptic curve cryptography would make more sense to be used only for infrequent but security-critical operations, like key establishment during the initial configuration of the sensor network.

In a Smart Grid for example, when a sensor node sends the sensed data to the base station (maybe a laptop computer or any interface-based system), the data must be made confidential through the route from the source node to the base station. But if the data is passed through the malicious node, it can read or modify the data. What we hope to achieve in future is a way to keep the data confidential from the source node to the base station at each step as follows.

- A malicious node can enter our network and can send forge or confused data to the base station to be pretend to be an authorized node.
- It can also modify, insert or delete the data during transmission impersonated as a legal node. An algorithm to prove the authentication and keep data integrity is to be in place here.
- Any unauthorized malicious node can send duplicate data and can attempt to repeat authorized data to the base station which is already send. Our protocol also protects replay attack.
- The sensor network must be robust menace if let a new node is added to the existing network, it should be added network securely.

ECC will minimize the above said attacks at the sensor network and prevent attacks that will affect confidentiality, authenticity, data integrity of data.

- Each sensor node has unique id.
- Sensor nodes are homogeneous and static.
- Attacks take a certain amount of time after a node has been deployed.
- Each sensor node has a randomly-generated hash bit that represents a state of the sending node, and is attached to every message sent, and changed to the next bit on the next message-sending.

A typical ECC algorithm may include two phases: after deployment of the sensor nodes and on addition of a new sensor node into the Smart Grid. Firstly, the base station selects a large integer q, which is either prime number p or an integer of the form 2^m and elliptic curve parameter a and b for following equation.

$$y^2 + xy = x^3 + ax^2 + b \tag{1}$$

This defines the elliptic group of points $E_q(a, b)$. The base station also picks a base point G from the above points whose order is a very large value n. The base station selects private value $n_1, n_2 \cdots n_N$ for sensor nodes 1, 2 $\cdots N$ respectively, which is less than n for every station and for itself also. These are the private keys for each of the sensor nodes and base station [48]. The base station should generate public keys for each of the sensor nodes and for itself by following equation:

$$P = n * G \tag{2}$$

where n and P are the private and public values of the nodes.

After deployment of each sensor nodes, every node of our static network will broadcast their public value P to its neighbouring nodes with its id. In the algorithm generated in [48], every node calculates its secret key (that will be different for each pair) by using following hypothesis.

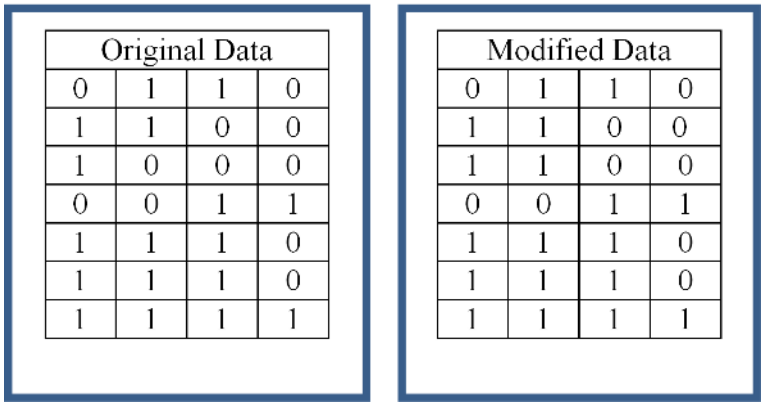
Let the second node be a neighbor of the first node, so by using Equation (1) and Equation (2), generate same key K (symmetric Key) at both ends.

$$K = n1 * p2(\text{at node 1}) \tag{3}$$

and

$$K = n2 * p1(\text{at node 2}) \tag{4}$$

Now every node has a secret key to exchange the message to each other with its id. This ensures our earlier discussed security attributes (confidentiality, data integrity and authentication) between the nodes. Then as first message every node sends a HELLO packet to its neighbours containing its id and a nonce starting with 1 and encrypted with respective key. Then the receiving node receives and decrypts the HELLO packet and store the "nonce" with id. For the next message between the nodes, every packet contains the "nonce" with an increment of one with the data so that the receiver can verify that the current data is not sent from a false node by comparing the previously stored bit of the Hash tag and making sure it has indeed changed to the next bit. The hashing function will detect single-bit changes, as shown in **Figure 5**, and so it can, as in our illustration above,



Original Data			
0	1	1	0
1	1	0	0
1	0	0	0
0	0	1	1
1	1	1	0
1	1	1	0
1	1	1	1

Modified Data			
0	1	1	0
1	1	0	0
1	1	0	0
0	0	1	1
1	1	1	0
1	1	1	0
1	1	1	1

Figure 5. Hashing detects single-bit discrepancies.

prevent a sybil replay attack.

On addition of a new sensor node in Smart Grid to a node that exits with the same values that is n_R, P_R and G, it exchanges the public value P_R and G to its neighbours. By using this method the neighbours generate the corresponding keys by using its previous value that is encrypted with its symmetric key.

4. Conclusions

The ECC algorithm depends on the effectiveness and difficulty of the computing discrete logarithms. This increases the strength.

In our future research works, we hope to bring forth a proposed scheme for access control in WSNs, as a continuation of current researchers' exertions towards that particular purpose.

References

[1] Sule, A.H. (2010) Major Factors Affecting Electricity Generation, Transmission and Distribution in Nigeria. *International Journal of Engineering and Mathematical Intelligence*, **1**.

[2] Azinge, E. (2012) Communique at the Round Table on Power Infrastructure, Investment and Transformation Agenda. http://www.nials-nigeria.org/round_tables/communique_on_power.pdf

[3] Punch (2012) Minister Orders Closure of Kainji Hydro-Power Station. http://www.punchng.com/ news/minister-orders-closure-of-kainji-hydro-power-station/

[4] Gungor, V.C., Lu, B. and Hancke, G.P. (2010) Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Transactions on Industrial Electronics*, **57**, 3557-3564. http://dx.doi.org/10.1109/TIE.2009.2039455

[5] George, E.O. and Oseni, J.E. (2012) The Relationship between Electricity Power and Unemployment Rates in Nigeria. *Australian Journal of Business and Management Research*, **2**, 10-19.

[6] Bello, O. (2012) Vandals Threaten Power Supply. Business Day. http://www.business dayonline.com/NG/index.php/power/42880-vandals-threaten-powernsupply

[7] Abawajy, J. and Robles, R.J. (2010) Secured Communication Scheme for SCADA in Smart Grid Environment. *Journal of Security Engineering*, **7**, 575-584.

[8] Sydelle, S. (2009) A Smart Grid for Nigeria's Energy Woes. http://www.nigeriancuriosity.com/2009/10/smart-grid-for-nigerias-energy-woes.html

[9] Kim, T.-H. (2011) Securing Communication of SCADA Components in Smart Grid Environment. *International Journal of Systems Applications*, *Engineering & Development*, **5**, 135-142.

[10] US Department of Energy (2009) Study of Security Attributes of Smart Grid Systems—Current Cyber Security Issues. US Department of Energy, Washington DC.

[11] ASAP (2008) AMI System Security Requirements. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf

[12] CEA (2010) The Smart Grid: A Pragmatic Approach. A "State-of-Play" Discussion Paper Presented by the Canadian Electricity Association. http://www.electricity.ca/media/SmartGrid/SmartGridpaperEN.pdf

[13] Meserve, J. (2009) "Smart Grid" May Be Vulnerable to Hackers.

http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/?iref=mpstoryview

[14] Fehrenbacher, K. (2009) Securing the Smart Power Grid from Hackers. http://www.businessweek.com/technology/content/mar2009/tc20090320_788163.htm

[15] Cavoukian, A. (2009) Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. http://www.privacybydesign.ca/content/uploads/2009/11/pbd-smartpriv-smartgrid.pdf

[16] Polulyakh, E. (2012) Smart Grid & Common Criteria. BKP Security, Inc. http://yourcreativesolutions.nl

[17] Fan, Z., Kalogrisis, G., Efthymion, C., Sooriyabandara, M., Serizawa, M. and McGeehan, J. (2009) The New Frontier of Communications Research: Smart Grids and Smart Metering. *Proceedings of the* 1*st International Conference on Energy-Efficient Computing and Networking*, 115-118.

[18] Flick, T. and Morehouse, J. (2011) Attacking Smart Meters. In: Flick, T. and Morehouse, J., Eds., *Securing the Smart Grid*, Syngress, Boston, 211-232.

[19] Akella, R., Tang, H. and McMillin, B.M. (2010) Analysis of Information flow Security in Cyber-Physical Systems. *International Journal of Critical Infrastructure Protection*, **3**, 157-173. http://dx.doi.org/10.1016/j.ijcip.2010.09.001

[20] Lee, A. and Brewer, T. (2009) Smart Grid Cyber Security Strategies and Requirements. NISTIR 7628, NIST.

[21] Open, S.G. (2008) AMI Security Requirements. Technical Report, AMI-SEC TF, OpenSG.

[22] Saranya, P. and Kundur, D. (2012) Bloom Filter Based Intrusion Detection for Smart Grid. http://www.comm.utoronto.ca/~dkundur/pub_pdfs/ParKunCCECE12.pdf

[23] Alese, B.K. (2004) Design of Public Cryptosystem Using Eliptic Curve. Ph.D. Thesis, Federal University of Technology, Akure.

[24] Adetunmbi, A.O., Falaki, S.O., Adewale, O.S. and Alese, B.K. (2008) Intrusion Detection Based on Rough Set and K-Nearest Neighbour. *International Journal of Computing and ICT Research*, **2**, 60-66.

[25] Gams, M. and Tušar, T. (2007) Intelligent High-Security Access Control. *Informatica*, **31**, 469-477.

[26] Ambler, S.W. (2012) Implementing Security Access Control. http://www.agiledata.org/essays/accessControl.html

[27] Ogundele, O.S. (2011) Design of a Multi Access Control System for Delegation Based on Attributes, Separation of Duty and Trust. Ph.D. Thesis, Department of Computer Science, Federal University of Technology, Akure.

[28] McDaniel, P. and Mclaughlin, S. (2009) Security and Privacy Challenges in the Smart Grid. *IEEE Security and Privacy*, **7**, 72-74. http://dx.doi.org/10.1109/msp.2009.76

[29] ABC News (2008) ABC News Channel. US. http://abcnews.go-com/technology/pcworld/story?id

[30] Intel (2008) Computing Technologies for the Smart Grid. http://www.intel.com/content/www/us/en/energy/energy-intel-technologies-smart-grid-brief.html

[31] Ling, A.P.A. and Masao, M. (2011) Grid Information Security Functional Requirement: Fulfilling Information Security of a Smart Grid System. *International Journal of Grid Computing & Applications* (*IJGCA*), **2**, Published Online. http://dx.doi.org/10.5121/ijgca.2011.2201

[32] Ling, A.P.A. and Masao, M. (2011) Selection of Model in Developing Information Security Criteria on Smart Grid Security System, Smart Grid Security and Communications. 2011 9*th IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops* (*ISPAW*), Busan, 26-28 May 2011, 91-98. http://dx.doi.org/10.1109/ispaw.2011.12

[33] Vieir, M., Vieir, J. and Madeir, H. (2008) Towards Data Security in Affordable Data Warehouses. 7*th European Dependable Computing Conference* (*EDCC*-7), Kaunas, 7-9 May 2008.

[34] Anderson, C. (2007) Information Security and Availability: The Impact of Training on IT Organizational Performance, White Paper, No. 20692, 2. http://eval.symantec.com/downloads/edu/Impact_of_Training_on_Organizational_Performance.pdf

[35] AICPA (2006) Trust Services, Principles, Criteria and Illustrations. http://www.webtrust.org/principles-and-criteria/item27818.pdf

[36] Wright, A.K., Kalv, P. and Sibery, R. (2010) Interoperability and Security for Converged Smart Grid Networks. http://www.smartgridnews.com/artman/uploads/1/wrigth_gi10.pdf

[37] CSWG (2010) Smart Grid Interoperability Panel—Cyber Security Working Group Standards Review. http://members.sgip.org/apps/group_public/download.php/2873/NAESB%20REQ%2021%20SGCC%20Review.pdf

[38] White Paper (2009) Cyber Security for Smart Grid System, 9. http://www.aesieap0910.org/upload/File/PDF/4-Technical%20Sessions/TS18/TS1806/TS1806_FP.pdf

[39] Wiki (2012) Cybersecurity. http://en.wikipedia.org/wiki/cyberwarfare

[40] Trèek, D. (2003) An Integral Framework for Information Systems Security Management. *Computers & Security*, **22**, 337-360. http://dx.doi.org/10.1016/S0167-4048(03)00413-9

[41] Sarka, K.R. (2010) Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures. *Information Security Technical Report*, **15**, 112-133.

[42] Colwill, C. (2009) Human Factors in Information Security: The Insider Threat—Who Can You Trust These Days? *Information Security Technical Report*, **14**, 186-196. http://dx.doi.org/10.1016/j.istr.2010.04.004

[43] Raymond, D.R. and Midkiff, S.F. (2008) Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing*, **7**, 74-81. http://ieeexplore.ieee.org

[44] Newsome, J., Shi, E., Song, D. and Perrig, A. (2004) The Sybil Attack in Sensor Networks: Analysis & Defenses. *IPSN*'04, *Proceedings of the* 3*rd International Symposium on Information Processing in Sensor Networks*, Berkeley, 26-27 April 2004, 259-268. http://dx.doi.org/10.1145/984622.984660

[45] Sheela, D., Srividhya, V.R., Asma, B.A. and Chidanand, G.M. (2012) Detecting Black Hole Attacks in Wireless Sensor Networks Using Mobile Agent. *International Conference on Artificial Intelligence and Embedded Systems* (*ICAIES*' 2012), Singapore, July 15-16, 45-48.

[46] Singh, V.P., Sweta, J. and Jyoti, S. (2010) Hello Flood Attack and Its Countermeasures in Wireless Sensor Networks. *IJCSI International Journal of Computer Science Issues*, **7**, 23-27.

[47] Xu, Y., Chen, G., Ford, J. and Makedon, F. (2007) Detecting Wormhole Attacks in Wireless Sensor Networks. *Critical Infrastructure Protection*, *International Federation for Information Processing*, **253**, 267-279. http://dx.doi.org/10.1007/978-0-387-75462-8_19

[48] Ahmad, S., Rizwan, B.M., and Abbas, Q. (2010) Energy Saving Secure Framework for Sensor Network Using Elliptic Curve Cryptography. IJCA Special Issue on "Mobile Ad-Hoc Networks", 167-172.