Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 182 (2021) 46–55

Procedia Computer Science

www.elsevier.com/locate/procedia

17th International Learning & Technology Conference 2020

# 5G-Wireless Sensor Networks for Smart Grid- Accelerating technology's progress and innovation in the Kingdom of Saudi Arabia

Charles Rajesh Kumar.J[a*], Ahmed Almasarani[a], M.A.Majid[a]

[a]*Department of Electrical and Computer Engineering, College of Engineering, Effat University, Jeddah, Saudi Arabia*

**Abstract**

The constant energy requirement was a crucial concern in today's smart grid era, which needs tremendous attention. New wireless networking technologies should be integrated into the grid to achieve more distributed generation and energy storage. Advancements in wireless sensor networks (WSN) and embedded systems have enabled the implementation of smart grid monitoring and automation systems at low cost. The incorporation of fifth-generation networks (5G) in a smart grid would create novel business models of "edge" and "fog" technology at the utility side, accompanying with smart-control and automation. Nonetheless, WSN's increased implementation also introduces impediments to safety, particularly relevant to confidentiality, accessibility, and safety management, creating both utilities and customers' unpredictable expenditure and catastrophe. In this paper, a comprehensive overview of the communication and computing aspects of 5G network infrastructure is provided and discussed how they can be beneficial in promoting advanced smart grid systems in the Kingdom of Saudi Arabia. Besides, this paper discusses the smart grid, current security issues surrounding machine-to-machine information on the smart grid, and solutions available to identify and avoid cyber threats.



*Keywords:* 5G; IoT; Saudi Arabia; Smart Grid; Energy efficiency; Wireless Sensor Networks; Challenges; Cyber Security

## 1. Introduction

The traditional grid is fitted with electromechanical sensors and relays, and the smart grid uses state-of-the-art digital relays and other sensors. The traditional grid communicates one way. Nevertheless, the smart grid uses digital communication in two ways. The traditional grid is based on the centralized generation, and the smart grid utilizes distributed generation. The traditional grid will have minimal sensors, while the whole smart grid will have sensors. Monitoring power and fault-related issues in the traditional grid are done manually, but it is a self-monitoring system in the smart grid. Fault in the conventional grid is restored from the control center, but it is a self-healing process in the case of a smart grid. When an outage happens in traditional systems, this produces a catastrophe. But in the case of the smart grid, an adaptive islanding option is available. Conventional grid control is minimal, and smart grid control is widespread. The traditional grid is based on massive centralized production, and smart grids deal with small distributed sources of production. The primary goal of the traditional grid is to implement electricity production to satisfy the need for energy. It necessitates smart grids to adjust requirements based on the possible production, and consequently, for the sensing and control of complete modes of contact, extremely reliable communication linking the distribution, and the transmission is required **[1-4].**

A smart grid comprises of sensors, smart-meters, extensive data management, and surveillance devices **[5–10] that** are needed to make electrical utilities more sustainable. The main challenge is to manage remote contact among various head-end systems attached to smart-meters. A network of information systems is required, which covers all consumer equipment and services linked to substations. It supports efficient communication systems with the necessary system analysis that is a critical component of smart grid functionality **[11-12].** For numerous purposes and


10.1016/j.procs.2021.02.007

in distinguished applications with lower cost-effectiveness, wireless communications are generally favored over wired communications. It strengthens connectivity and offers promptly available connections, even those in remote locations. Several factors exist to count when determining a proper, stable communication system, such as operational expenses, environmental impacts, and resource availability **[13-15].** WSN's interactive, minimal-cost architecture provides considerable benefits compared to conventional communication technologies used in today's electrical systems. WSNs have recently been widely acknowledged as a promising technology that can boost different aspects of today's electrical systems, including production, distribution, and utilization, rendering them a critical component of the smart grid, the next-generation electrical power network.

Nonetheless, in smart grid implementations, harsh and dynamic electrical power network conditions present significant challenges in the efficiency of WSN communications. The implementation of WSNs in smart grids, however, brought new challenges **[16-20**] primarily because of the features of the electrical grid. For example, if attackers disrupt the grid at a later date from a remote location, cascading-failure-induced disasters can happen. The privacy data of smart grid customers could be unlawfully accessed through the wireless sensing network. The adversary could also compromise selected nodes in a network with tactical delay tolerance, and therefore, the Supervisory Control and Data Acquisition (SCADA) system's vital mission fails. Any of these forms of attack can pose a severe threat to the grid, and without energy, millions of houses could be left, and industries could be halted. Besides, power grids are a significant resource for the defense of the nation. A safe wireless ad hoc and high-capacity sensor network communication must be addressed to guarantee a secure and efficient smart grid.

As a result, standard WSN interaction protocols have been shown to be ineffective, and a number of recent research projects have been committed to improving them. This paper provides a detailed overview of relevant literature, addresses research problems that are still open, and identifies the most growing smart grid validation platforms to test WSN communications. We trust that this review will open the way for Saudi Arabia's smart grid research community to (i) understand critical concepts of smart grid communications cantered on WSN, (ii) recognize gaps and offer relevant contributions in this timely and exciting field and (iii) choose a suitable testing platform to validate the ideas suggested.

## 2. Smart Grid and 5G network

Cellular network technology of the fifth-generation (5G) has recently been promoted in several countries worldwide, Because of its significant benefits over previous generations (1G-4G) in terms of transfer speed, robustness, safety, energy consumption, and the number of connections **[21]**. The 5G electromagnetic wave frequency spectrum can reach hundreds of GHz, which is significantly higher than the current 1G -4G frequency spectrum **[22]**. 5G wavelength is, therefore, smaller, with more extensive data transfer capacity (larger bandwidth). 5G technology is regarded as the most significant catalyst for the developing global Internet of Things (IoT) **[23]**. Digitalization reshapes the energy sector's landscape. The need for increased energy efficiency, improved process control, and better customer experience is pushing the IoT devices to be adopted, which in effect requires state-of-the-art networking technologies to guarantee smooth data exchange **[24-31].** Communications related to utilities are one of the most demanding of IoT applications, with millions of devices that need to be connected wirelessly to an extreme level of safety and reliability.5G would seem to shape the energy sector's future. **Table.1** provides a comparison of the leading 4G and 5G parameters.

**Table 1.** Fifth-generation of technology for wireless networking

| Key parameters | 4G | 5G |
|---|---|---|
| Latency | 10 ms | <1 ms |
| Data traffic | 7.2 Exabyte/month | 50 Exabyte/month |
| Peak data rates | 1 Gb/s | 20 Gb/s |
| Available spectrum | 3 GHz | 30 GHz |
| Connection density | 100 thousand connections/$km^2$ | 1 Million thousand connections/$km^2$ |

There are strict infrastructure requirements in connectivity and data transmission for 5G and IoT applications on an industrial scale. In addition to the issue of how to maximize 5G capacity, early adopters concentrate on the following

requirements for this emerging networking technology: 1000x bandwidth, 99.99 percent availability, 1ms latency, up to 1000x quantity of combined devices, up to 10 Gbps data rate, up to ten-year battery life, hundred percent coverage, ninety percent reduction in network energy usage. First of all, 5G energy efficiency would minimize costs and improve decision-making with information insights, and provide the ability to communicate virtually any device over a considerable distance and provide control over hard-to-reach facilities to avoid life-threatening incidents. **Fig.1** reveals sectors that benefit the most from 5G **[32].**

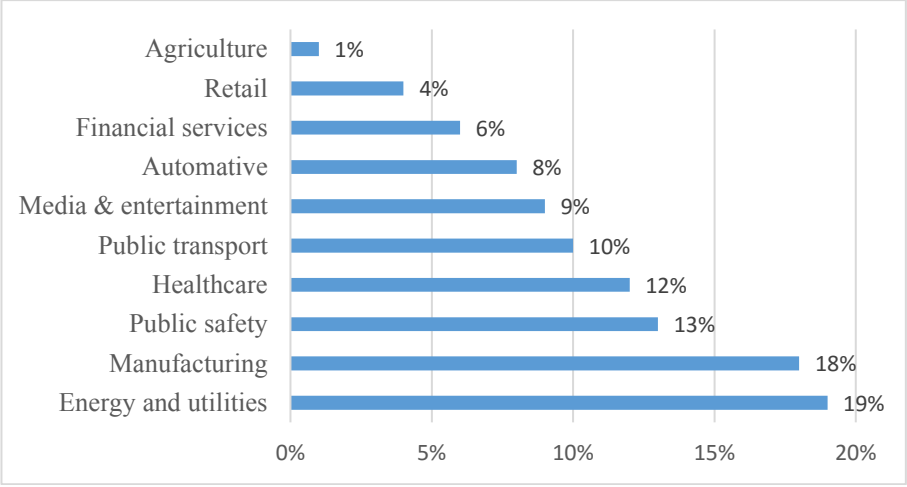


**Fig. 1**. Industries that are most effective from 5G **[32]**

5G wireless technology is going to pave the way for innovative features and more capable smart grids. New 5G mobile networks will help unite previously separated devices into new smart grids to monitor their energy requirements precisely and to accurate forecasting. Energy demand management will be much easier and more effective, requiring less capital, as the smart grid balances power loads, decreases demand spikes, and eventually reduces energy costs. Based on data collected, large cities will be able to plan their power infrastructure, invest less, and minimize downtime. A smart grid combines conventional grid technology with communication and information control defined by performance, cleanliness, privacy, and security. 5G will be a crucial ingredient in smart grid technology development, to allow the grid to adapt better to renewable energy dynamics and distributed generation. Since renewable resources such as solar and wind are intermittent, integrated monitoring and control of the grid will be necessary. In addition to integration with substation automation, different energy flows are regulated, and standby capacity is designed to complement intermittent generation. Smart Grid capabilities can make it easier to track, manage, and endorse bi-directional power flows. Most of the spending is in three major categories when it comes to energy: smart grids, smart metering, and smart homes.

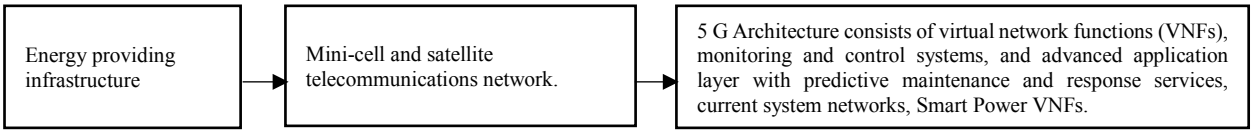


**Fig. 2.** Smart grid framework for energy

The energy supplying infrastructure consists of the hydro-electric plant (extra-high voltage 265 to 275 W), power plant (110kV), wind farm, PV parks (distribution grid), and smart-meters. The telecoms layer consists of a cellular network with a satellite network and mini-cell network, as shown in **Fig.2**. 5G helps to handle efficiently, and cost-effective, energy production and transmission. Via low-cost 5G connections, most unconnected energy-consuming devices are expected to be incorporated into the grid, also–precise monitoring of these devices to offer a better prediction of energy requirements.

## 3. Smart Grid and Wireless Sensor Network (WSN)

In the 21st century, WSNs were widely regarded as essential technology, deployed in massive applications varying from monitoring, control, and detection. WSN technology is a viable technology to achieve smart grid monitoring and control that is seamless, energy-efficient, secure, and low price. WSNs are implemented throughout the smart grid process, i.e., production, transmission, and distribution, as well as the consumer level. Some of the features provide control and load management, automatic wireless meter reading, diagnostic failure of devices, remote monitoring, and detection of faults, advanced metering systems, and control of residential power.

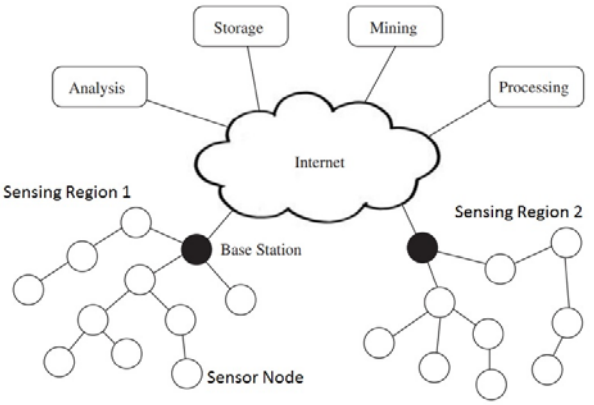


**Fig.** 3 The architecture of Wireless sensor networks

The architecture of the WSN hardware consists of a base-station which function as a portal among the end-user and sensor-nodes. Base-station collects sensor-node information. They follow single-hop and multi-hop communication. The base station will transmit data to the server from the WSN, which is shown in **Fig.** 3. A sensor-node consists of four key components, such as a transceiver unit, a sensor unit with ADC, the central **processor,** and a power supply unit **[33-34].** ADC digitizes the sensor information, and the processor analyzes the results. Optimized routing-protocols are structured to respond immediately and identifying potential paths for transmitting the digital signal to the next node. Data processing and node management is the responsibility of the processing unit. The transceiver comprises of RF-transmitter and RF-receiver and connects the nodes via the communications network. The power supply unit provides constant energy for nodes. Currently, energy harvesting helps power supply systems. The power supply has a significant impact on the node's lifetime **[35].** The modern industrial and smart grid communication systems are implemented with WSNs that are composed of many sensor nodes, and they have several features from conventional sensors. The expected characteristics of WSN used in the smart grid are listed below: **[36 -39]:**

**The capacity of computing**: Replacing the battery or removing the unit expense is higher than the sensor node cost. The computing power of sensors in the smart grid is confined, and space for memory and storage are also minimal.

**Power for the battery**: Losing the power source would result in nodes being disabled. The protocols and algorithms used should also reduce the energy consumption of the system.

**Capacity for communication**: Because of limitations on resources, in a smart grid, sensor-nodes are confined in their overall connection distance. Unpredictable weather conditions, such as wind speed, rainfall, etc. that can lead to severe network performance deterioration.

**Possibility of adaptation:** WSN's power supplies fail in several applications sooner than the estimated lifespan. WSNs should, therefore, be able to adapt and resolve issues and continue to do their job. WSNs would, for example, can be reconfigured and adjusted to varying circumstances dynamically. It is, however, an open topic of research to develop an extraordinarily adaptable and self-configurable WSN.

**Organization of oneself**: WSN have self-organizing features, and WSNs do not need a pre-established network infrastructure. Sensor-nodes must be able to work and function efficiently in a cooperative manner.

**Communication via multi-hop:** Multi-hop communication is utilized for reducing power utilization and increasing the lifespan of the WSN network. Sometimes using gateways and routers, a node should connect to a non-direct neighbor node to transmit the data with the support of intermediate nodes.

## 4. Challenges of WSN in Smart Grid applications

WNS is a core part of the smart grid's self-healing capabilities because WSN can self-organize and self-heal. WSN can build a network topology requiring no human involvement and prior knowledge of topology. WSN can recover from faults through the use of redundancies in software and hardware. WSN's limitations and Heterogeneous system of communication for the smart grid lead to certain obstacles in the implementation and operation of WSN, which is displayed in **Table 2 [40-45].**

**Table 2**. The WSN's challenges in the deployment of smart grids

| Hurdles | Overview |
|---|---|
| Extreme environmental factors | Wireless sensor nodes can be exposed to extreme environmental factors that can trigger wireless sensor node failure. |
| Various topologies of the network | Heterogeneous network topologies due to different features in the energy distribution network and sensor-node failure can pose technical challenges in sensor-node design |
| Reduced capability | Diminished capacities in processing and storage cause different difficulties in developing and deploying WSNs. |
| Bit-error rate and noise | Increased rates of bit-error are found in communication systems due to increased levels of noise. It requires different systems for error detection and correction. Error detection and correction require more storage and processing facilities, which challenge the design of the sensor network. |
| Sensor network safety and security | Wireless sensor network security is an essential and vital prerequisite. The sensor-nodes should be protected from external manipulation to hacking (an effort to misuse) for the steady operation of the several smart grid application. It is physical manipulation to strike a WSN network by grabbing any of the nodes, breaking into the node. |
| Service quality requirements for the environment of smart grids | Reliability of data transmission, latency, high-data-rates, consistency, and integrity are critical to smart grid applications ' service quality requirements. Wireless sensor networks must meet these criteria for different applications to be successfully implemented. |

## 5. Attacks on WSN in Smart Grids

A large number of sensor nodes are mounted in the smart grid to collect the data in real-time. WSN-based monitoring systems are implemented in the harsh and complex conditions of the electrical power grid. Principally, they are subjected to cybersecurity threats of traditional WSN, extending from simple attacks such as modification, spoofing, eavesdropping, replaying, traffic analysis, man-in-the-middle, and blocking to more to sophisticated attacks such as routing attacks, Sybil attacks, and selective forwarding and hello floods. Cyber-attacks on various layers of WSN are given below:

**Physical layer:** The principal functions at the physical layer are 1.the selection of communication frequency, 2.generation of the carrier frequency, 3.detection of signal, and 4.encryption of data. Jamming and hacking are the two security attacks that can be carried out on this layer. Most types of devices function in the RF range of the sensor-node, and when these devices operate close to the WSN, they can produce large quantities of interference or noise. The airwaves may be distorted, resulting in a drop in the signal-to-noise ratio. This can interrupt or stop the WSN node operation in the area of the attack. Data tampering is done by using different types of hacking methods to obtain vital data (e.g., encryption key). The sensor–node position may be modified by the attacker; the attacker could introduce a fraudulent node to control or monitor other sensor-nodes of the smart grid. The sensor-nodes deployed in remote locations have more chances of hacking attacks.

**Data Link layer: The data link layer's main task is to manage errors of transmission,** data flow control, offer a distinct network interface. Further, more logical link control and media access control is done by this layer, which knows the starting and end of the bit-stream. This layer is attacked using a "spoofing attack" in which the attacker effectively masks information as another node achieves an unlawful benefit. One of the security weaknesses of the data link layer is the risk of inducing collisions. In spoofing an attacker continues to send vast numbers of messages violates the usual protocol interaction in a premeditated way. The possibility of collisions is the safety vulnerability of this layer, and it will result in nodes being depleted and scarce resources being consumed because the nodes are forced to react to the messages obtained.

**Network Layer**: To set up a network between the nodes and routing data to the appropriate endpoint or location is the principal responsibility of the network layer. This layer is attacked using a "denial of service" (DoS) attack. The DoS attack aim is to shut down the network or its regular operation and make it unavailable for the user. Furthermore, the layer is attacked using a "Sybil attack." This attack's main aim is to isolate the nodes by modifying routing and confusing the routing protocols where a node reports several false identities to destroy a network.

**Transport Layer:** It is the responsibility of the transport layer to handle end-to-end communications and to ensure secure connectivity. This layer is attacked using a "Flooding" attack. The attack aim is to make the network's resources unavailable or exhaust by generating false messages or a considerable number of requests to raise network traffic and to degrade the node.

## 6. Security in 5G based Smart Grid Networks

In addition to the apparent benefits of utilizing 5G technologies and WSN, the smart grid is further exposed to the attack by cybercriminals **[46].** Safety is the smart grid system's most influential affair and comes with three principal objectives, such as service availability, data protection, shared information integrity. A smart grid has a broad spectrum of drawbacks, as it has an extensive infrastructure. The lack of access to services initiated by cyber-attacks can lead to a decrease in demand **[47].** The smart grid network incorporates improvements and changes which make traditional energy network complex, which is susceptible to various types of attacks. The attackers quickly access the network, making the system inaccessible or disable. Furthermore, integrity and data privacy during transmission are violated. The following are the various severe vulnerabilities in smart-grids **[48]:**

**The confidentiality of the client:** The smart-meters provide access to the private data and activities of the customer, such as the time of use and time of non-use, customer's location, and availability, etc.

**A considerable number of points of access:** The smart grid uses many devices to manage power supply and network requirements. The attackers quickly access and manipulate these devices since it is a difficult task to handle such a vast range of devices.

**Physical Security:** Smart-network connections found in remote locations face physical safety concerns. Such insecure places require independent, local-controlled security mechanisms.

**Frequent updates of components of the network:** In a grid, the life of the components of IT is reduced. The IT components need to be upgraded frequently, and seldom upgrading, or updates are not compatible with specific hardware, software, and drivers on the device of the smart grid or the smart-meter.

**Complete trust between conventional energy devices:** If a device's output in a smart grid serves as an input to the next device, incorrect data (Spoofing attack on cascaded device) will be causing the entire network to collapse.

**Differences between the teams:** Different teams are working on the smart grid at different locations. The inconsistency and coordination differences between teams lead to bad decisions and create physical security loopholes.

**IP and commercially available off-the-shelf software and hardware:** Compatibility among various devices is achieved through the internet protocol. IP spoofing and denial of service is another concern related to the internet protocol.

**More interested parties (Stakeholders):** A significant number of stakeholders and a lack of knowledge among stakeholders involved in the smart grid also give rise to security challenges. The unauthorized access and malicious code are both dangerous for the functioning of stable power systems. With a large number of harmful cyberattacks on the networks, it is of great importance to identify potential weaknesses. An intruder may be in-house or outside of the network. The researchers categorized cyber attackers into groups **[49-53]:**

**Non-Malicious invaders:** The attackers consider the smart grid security system as a mystery or puzzle and attempt to solve it by decoding using their rational principles.

**Customers**: In particular, disgruntled customers who are motivated by anger and hatred towards the providers of services or customers.

**Subversives**: Targets smart grids intending to reduce the service or collect critical information.

**Internal Workers (Employees):** Untrained staff or disgruntled staff who are disrespectful to other customers or service providers.

**Competitors**: They attack one another for personal gain and often to threaten counterpart assets.

**Use of malware**: An attacker could use malware to collapse smart-meters or significant resources. Often, malware can change or remove confidential information.

**Unauthorized access to information:** The server should have a proper security mechanism using databases to verify the validity of the logins. If not, the network can be accessed easily by unauthorized attackers, and they may manipulate the resources.

**Playback:** To create an unwanted effect, an attacker may send false messages or retransmit the same message many times. There is an adverse effect on these fake messages. These can unnecessarily involve the receiver or may overwhelm the receiver resulting in the entire interaction being unreliable or slowed down.

**Traffic investigation:** The attackers investigate the network traffic and analyze the routing system of data packets to reach the destination. An attacker can obtain relevant information such as a fundamental smart grid framework, quantity of energy use, cost, etc. through such an attack.

## 7. Suggested cybersecurity strategy for 5G based Smart Grid Networks

Smart grids use networking technologies that make them exposed to dangerous cyber-attacks. It is a tempting target for advanced and well-equipped hackers because the power grid is a critical infrastructure. Cyber-attacks are usually based on malware that has to interact with a governing party over the network to coordinate and propagate [**54].** Security should be included in every phase of the life cycle of the system development, from the design phase through installation, maintenance, and disposition. Critical application systems have to endure cybersecurity events without any loss of critical function. To secure networks and devices from cyber threats, we concentrated on evaluating interdependencies to evaluate their importance, dangers, mitigating factors, and possible security strategies to be implemented which are listed below:
**Updates of security**: Constant and timely upgrades in enterprise and industrial networks for devices, eliminate vulnerabilities, and reduce opportunities for attackers.
**Administration of users**: All users are restricted to areas appropriate for their position, including administrators.
**Rule on passwords:** Clear password policy allows the use of long non-repeating passphrases with high entropy.
**Anti-virus**: Use advanced anti-virus software focused on heuristics and services of remote credibility.
**Segmentation of the network:** Separate subnetworks with different goals, e.g., there is segmentation between the administrative network and the system of industrial control.
**Limiting remote access**: Rigorously controlled and limited to trusted individuals for remote access.
**Strict rules on firewalls**: By default, all access is forbidden, except for white-listed hosts and services that safeguard users from threats to the internet.
**Critical service decentralization**: Decentralization increases resistance to assaults. Nonetheless, specific countermeasures, such as infected removable drives, are needed to counteract propagation techniques that are not dependent on a functioning network.
**Software dimensioning for potential software updates**: For more than 10 years, smart grid devices have been in service. Whenever resource-constrained hardware or software is integrated as part of a modular design into modern equipment, in the case of sophisticated attacks, the security of the entire system may be compromised. These devices are therefore prepared for future requirements as well as provide adequate resources to support updates.
**User learning**: User training, which protects against many simple access vectors, is one of the most important countermeasures. This can significantly hinder propagation in combination with strong passwords.
**Guaranteeing data security, confidentiality, and accessibility:** packet-integrity-attacks or sniffing are prevented by implementing standard protocols.
There are three phases in the strategy: pre-attack, under attack, and post-attack. Solutions are described in terms of safety protocols, security technology, cryptography, and other countermeasures to cyber-attack.

**Pre-attack:** The three primary function of this stage is 1.encryption and decryption using cryptography techniques, 2.protecting the credibility, privacy, and functionality of the networks using network-security, 3. Protecting devices and information stored. Secure protocols such as IDS, SIEM, DLP, and secure DNP3 can be used for these purposes. IDS is an intrusion-detection system, SIEM is security-information and event-management, DLP is data-leakage protection, and DNP3 is distributed network protocol. DNP3 is suitable for low bandwidth WAN communication, and this makes it ideal for power grids and other SCADA systems, such as oil and gas pipeline management systems. DNP3 communication is used in the smart grid to communicate between the controller devices. Each substation is managed by a SCADA system that communicates on the DNP3 protocol on the Internet/IP. Furthermore, compliance checking and diversity-technique are also employed. Data from all devices in the network, such as network flow, operating system logs, and application logs are managed and aggregated by SIEM. A centralized server will then monitor and process the information gathered to identify every possible risk or disruptive network behavior. DLP helps to track and avoid sensitive information vulnerabilities, intelligence gathering, or unintended destruction, and also prevents data loss or theft across the network.

Secure-sockets-layers (SSL), Transport-layer-security (TLS), DNP3, Internet-protocol-security (IPsec) can also be used to improve network security in addition to these security systems. Encryption processes are designed to ensure

the privacy, integrity, and non-repudiation of the information. Advanced encryption standard and data encryption standard are the most commonly utilized algorithms which use symmetric encryption. On the other side, asymmetric key encryption utilizes two keys for encryption and decryption of data: a private-key and public-key. The selection of symmetric and asymmetric key encryption relies on many determinants, such as scalability considerations, capacity for computing resources, and multicast support. Especially for the power system, several key management mechanisms were proposed for safe SCADA communication: 1.SKMA, 2.SKE, 3.ASKMA, 4.ASKMA+, 5.SKMP, 6.HSKMA etc. SCADA is supervisory-Control and data-acquisition, SKMA is SCADA key-management-architecture, SKE is Sandia-key-management, ASKMA is advanced-key management-architecture, SKMP is SCADA-key-management-protocols and HSKMA is hybrid-key-management-architecture. The automated compliance check tool conducts a test against all elements of the smart grid to confirm that the configuration of every system is updated, particularly the firmware of the system and the existing configuration file. Since the smart grid components are intimately attached and vulnerability in an individual element can endanger the whole operation, and a compliance screening is also an essential tool for this purpose. Diversity technique is used to restrict a large-scale assault in smart-meter firmware.

**Under attack**: The main function of this stage is to detect cyber-attack and avoidance of the attack. During each task, it is possible to use several methods and techniques to detect malware and then implement active counter initiatives. All implemented security technologies, including SIEMS, DLP, and IDS, are suggested during the identification of the attack. But most of these methods, such as IDS, have a variety of shortcomings and have to be improved. IDS is a commonly used IT network security system that is utilized in smart grid networks. IDS will be necessary to detect attackers targeting the smart grid network. A smart grid distributed intrusion detection system **[55]** may be utilized in all levels of the smart grid such as wide-area-network, home-area-network, and neighborhood-area-network. The system is based on data mining algorithms such as an artificial immune system based support vector machine method. The NSL KDD dataset is used to test the effectiveness, and the detection of malicious traffic has achieved satisfactory results **[56].** Once the attack is identified, the pushback and reconfiguration methods can be used to minimize the DoS attack **[57].**

**Post-attack**: The post-attack duration is a crucial step if an attack is not detected **[58].**First, determining the entity that is engaged in the cyber-attack is critical. The signature-based intrusion detection system, database systems, and antivirus and protection measures will then be updated by discovering from threats and by protecting the smart grid from possible cyber-attacks. Cyber-security forensic investigation is the leading post-attack method used. Smart grid forensic analyses obtain, examine, and intercept digital data to classify the individual participating in the situation. They are also helpful in identifying and addressing the smart grid's cyber and physical vulnerabilities to prevent possible attacks. Furthermore, forensic smart grid analysis plays a crucial role in investigating cyber-crimes such as cyber terrorism, hacking, digital espionage, viruses, infringing the security of customers, exploiting the activity of the smart grid, and attempting to steal vital information such as intellectual property and country secrets **[59].**

## 8. Conclusion

A comprehensive summary of the new 5G technologies is presented in this work to develop smart grids as a future power arena. Smart grids have been observed to present significant and complex obstacles to 5G technology. A secure network of telecommunications and the sharing of information is needed to manage the elements of a smart grid. The network of telecommunications is, therefore, an essential component of control systems, electrical distribution, and electrical transmission for the smart grid. The network of telecommunication must be efficient, stable, cost-effective, and resistant to transient power systems and external causes of electromagnetic interference. Implementation of 5G mobile communications technologies with high bandwidth capability, low latency, high performance, and broad coverage is tailored to smart grid requirements. Hence, 5G performs an essential role in fostering smart grid growth. The installation of exceptional sensors and computation methods, concurrently with the communication system support, is required to facilitate the monitoring and administration of the smart grid and provide the sizeable real-time information movement connecting controlled-equipment and the management system of distribution. The study addresses the design of a 5G smart grid requires, and the areas where the evaluation of the network can be performed. This work sets a starting point for the introduction of new-age 5G smart grid networks and sets a course for researchers in Saudi Arabia to focus on new smart grid technologies and to provide trendsetters for new energy domains globally. Furthermore, we have provided a broad overview of smart grid cybersecurity and discussed in detail the significant

cyber-attacks that threaten the technology, network, and device protocols. We also suggested a strategy consisting of several tools and mechanisms to resolve the vulnerabilities of potential components, identify malicious operations, strengthen network communication security, and protect the privacy of the customer.

## References


[1] Farhangi, H. (2010) "The path-of-the smart-grid." IEEE Power Energy Magazine 8:18–28.

[2] Tuballa, M.L, Abundo, M.L. (2016) "A review of the development of Smart Grid technologies." Renewable and Sustainable Energy Reviews 59: 710–725.

[3] Kabalci, Y. (2016) "A survey on smart-metering and smart-grid communication. "Renewable and Sustainable Energy Reviews "57:302–318.

[4] Ma, R.,Chen, H.H,Huang, Y.R.,Meng, W. (2013) " Smart grid communication: Its challenges and opportunities." IEEE Trans. Smart Grid 4: 36–46.

[5] Ma, K,Liu, X,Liu, Z,Chen, C,Liang, H, Guan, X. (2017) " Cooperative Relaying Strategies for Smart Grid Communications: Bargaining Models and Solutions." IEEE Internet Things Journal 4:2315–2325.

[6] Yan, Y, Qian, Y,Sharif, H,Tipper, D. (2013) "A survey on smart grid communication infrastructures: Motivations, requirements and challenges." IEEE Communications surveys and Tutorials 15: 5–20.

[7] Gungor, V.C, Sahin, D,Kocak, T, Ergut, S, Buccella, C,Cecati, C,Hancke, G.P. (2011) " Smart-grid technologies: Communication technologies and standards." IEEE Transactions on Industrial Informatics 7:529–539.

[8] Wang, W, Xu, Y,Khanna, M. (2011) "A survey on the communication architectures in smart grid." Computer Networks 55:3604–3629.

[9] Feuchtinger, U,Eger, K.,Frank, R.,Riedl, J. (2014) " Smart Grid Communication Architecture." MMB DFT 127.

[10] Zaballos, A,Vallejo, A, Selga, J.M. (2011) "Heterogeneous communication architecture for the smart grid." IEEE Network magazine 25:30–37.

[11] Werbos, P.J. (2011) "Computational intelligence for the smart grid-history, challenges, and opportunities." IEEE Computational Intelligence magazine 6:14-21.

[12] Sauter, T, Lobashov. (2011) "M. End-to-end communication architecture for smart grids." IEEE Transaction on Industrial electronics 58:1218–1228.

[13] Osseiran, A.; Boccardi, F.; Braun, V.; Kusume, K.; Marsch, P.; Maternia, M.; Queseth, O.; Schellmann, M.;Schotten, H.; Taoka, H.; et al. (2014) " Scenarios for 5G mobile and wireless communications: The vision of the METIS project." IEEE Communication Magazine 52:26–35.

[14] Erol-Kantarci, M., & Mouftah, H. T. (2011) "Wireless multimedia sensor and actor networks for the next generation power grid." Ad Hoc Networks (Elsiver) 9(4):542–551.

[15] Gungor, V. C., Lu, B., & Hancke, G. P. (2010) "Opportunities and challenges of wireless-sensor networks in smart-grid." IEEE Transactions on Industrial-Electronics 57(10):3557–3564.

[16] Gungor, V. C., Lu, B., & Hancke, G. P. (2010) "Opportunities and challenges of wireless sensor networks in smart-grid." IEEE Transactions on Industrial-Electronics 57(10):3557–3564.

[17] Gungor, V. C., Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., et al. (2013) "A survey on smart-grid potential applications and communication requirements." IEEE Transaction on Industrial Informatics 9(1): 28–42.

[18] Bilgin, B. E., & Çagri Güngör, V. (2012)" Performance evaluations of zigbee in different smart grid environments." Computer Networks, 56(8):2196–2205.

[19] Temel, c, Gungor, Vc, & Koçak, T. (2014) "Routing protocol design guidelines for smart grid environments." Computer Networks 60:160-170.

[20] Yigit, M., Yoney, E., & Gungor, V. (2013) "Performance of mac protocols for wireless sensor networks in harsh smart grid environment." First International Black Sea conference on communications and networking (BlackSeaCom) 50–53.

[21] M. Agiwal, A. Roy, N. Saxena. (2016) "Next generation 5G wireless-networks: a comprehensive-survey." IEEE Communications surveys and Tutorials 18 (3):1617-1655

[22] 5G network architecture-A high-level perspective, Huawei, 2016.

Available: https://www.huawei.com/minisite/g/img/G_Network_Architecture_A_High-Level_Perspective_en.pdf.

[23] M.R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, et al. (2016) "Internet-of-things in the 5G era: enablers, architecture, and business models." IEEE Journal on Selected-Areas in-Communications 34 (3):510-527.

[24] Charles Rajesh Kumar J, Kanagaraj M (2017) " Enhanced TACIT Algorithm Based on Charl's table for Secure Routing in NoC Architecture" Journal of Computational and Theoretical Nanoscience 14(12):5680-5685.

[25] Charles Rajesh Kumar,T.Vanchinathan (2015) "An improved fast mode decision algorithm for VLSI architecture implementation" The Optoelectronics and Advanced Materials-Rapid Communications 9(5-6):738-745.

[26] A.Muthukrishnan, J. Charles Rajesh Kumar, Vinod Kumar. D, Kanagaraj. M (2018) "Internet of image things-discrete wavelet transform and Gabor wavelet transform based image enhancement resolution technique for IoT satellite applications" Cognitive Systems Research 57:46-53. doi.org/10.1016/j.cogsys.2018.10.010.

[27] Charles rajesh Kumar, Aziza Ibrahim (2018) "VLSI design of energy efficient computational centric smart objects for IoT" 15th Learning and Technology Conference (L&T) Jeddah, IEEE Xplore digital library 129-138. doi: 10.1109/LT.2018.8368497

[28] Charles Rajesh Kumar.J, Vanchinathan.T and Karthik.K (2013) "Design of SerDes Transceiver with fixed and high throughput implementation on FPGA" Life science Journal, 10(2):394-398.

[29] Charles Rajesh Kumar J, K. Kharthik (2014) "Design of low-latency 4K HEVS using V-By-One HS Transmission" Research journal of recent sciences 3(8):111-118.

[30] Charles Rajesh Kumar J, Vinod Kumar D, Baskar D, Mary Arunsi B, Jenova R, M.A. Majid (2019) "VLSI design and implementation of High-performance Binary-weighted convolutional artificial neural networks for embedded vision based Internet of Things (IoT)" Procedia Computer Science 163:639-647. doi.org/10.1016/j.procs.2019.12.145.

[31] Charles Rajesh Kumar J, Mary Arunsi B, Jenova R, M.A. Majid (2019) "VLSI design of intelligent, Self-monitored and managed, Strip-free, Non-invasive device for Diabetes mellitus patients to improve Glycemic control using IoT " Procedia Computer Science 163:117-124. doi.org/10.1016/j.procs.2019.12.093.

[32] Ericsson Report – The 5G Business Potential: Second Edition

[33] H. Jin. (2010) "Handbook-of-Research on Developments and Trends in Wireless-Sensor-Networks: From Principle to Practice." Information Science Reference.

[34] N. V. Kirianaki, S. Y. Yurish, N. O. Shpak, and V. P. Deynega. (2002)" Data Acquisition and Signal-Processing for Smart-Sensors." Wiley.

[35] M. A. Matin. (2014) "Handbook of Research on Progressive Trends in Wireless-Communications and Networking." GI Global.

[36] L. Yong-Min, W. Shu-Ci, and N. Xiao-Hong. (2009) "The Architecture and Characteristics of Wireless-Sensor-Network." International Conference on Computer Technology and Development 561-565.

[37] I. M. M. E. Emary and S. Ramakrishnan. (2013) "Wireless Sensor Networks: From Theory to Applications." Taylor & Francis.

[38] B. A. Alohali and V. G. Vassialkis. (2015) "Secure and energy-efficient multicast routing in smart grids." IEEE Tenth International Conference on Intelligent-Sensors, Sensor-Networks and Information-Processing (ISSNIP) 1-6.

[39] Yuan Gao, Hong Ao, Zenghui Feng, Weigui Zhou, Su Hu, Wanbin Tang. (2018) "Mobile Network Security and Privacy in WSN"Procedia Computer Science 129:324-330.

[40] Mohammad Abujubbeh, FadiAl-Turjman, Murat Fahrioglu. (2019) "Software-defined wireless-sensor-networks in smart grids: An overview." Sustainable Cities and Society 51:101754

[41] Brak, M.E, Brak, S.E, Essaaidi, M, Benhaddou, D. (2014) "Wireless Sensor Network applications in smart grid." Proceedings of the IEEE International Renewable and Sustainable Energy Conference (IRSEC) 587–592.

[42] Zhang, Y, Li, X.; Zhang, S. Zhen, Y. (2012) "Wireless sensor-network in smart-grid: Applications and issue." Proceedings of the World-Congress on Information and Communication Technologies (WICT) 1204–1208.

[43] Erol-Kantarci, M, Mouftah, H.T. (2011) "Wireless Sensor Networks for smart grid applications." Proceedings of the IEEE International-Conference on Electronics, Communications and Photonics (SIECPC) 1-6.

[44] Erol-Kantarci, M, Mouftah, H.T. (2010)" Using wireless sensor networks for energy-aware homes in smart grids." Proceedings of the IEEE Symposium on Computers and Communications (ISCC) 456–458.

[45] Brak, M.E, Essaaidi, M. (2012) "Wireless sensor network in smart grid technology: Challenges and opportunities." Proceedings of the IEEE International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 578–583.

[46] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. (2006) "Wireless Sensor Network Security: A Survey." CRC Press.

[47] M. Healy, T. Newe, and E. Lewis. (2009) "Security for wireless sensor networks: A review." IEEE Sensors Applications Symposium (SAS), 80-85.

[48] De Dutta, S. & Prasad.R (2019) "Security for Smart Grid in 5G and Beyond Networks." Wireless Personal Communications 106(1): 261-273

[49] S. Clements, H. Kirkham. (2010) "Cyber-security considerations for the smart grid", IEEE Power and Energy Society General Meeting, pp. 1-5.

[50] I. Pearson. (2011) "Smart grid cyber security for Europe." Energy Policy 39(9):5211-5218.

[51] T Flick, J. Morehouse. (2010) "Securing the Smart-Grid: Next Generation Power Grid Security." Syngress (Elsevier).

[52] X Wang, P. Yi. (2011) "Security framework for wireless-communications in smart-distribution grid." IEEE Transactions on Smart-Grid 2(4): 809-818.

[53] Peter Eder-Neuhauser, et.al. (2017) "Cyber-attack models for smart grid environments." Sustainable Energy, Grids and Networks 12:10-29.

[54] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez. (2015) "Data-stream-based intrusion-detection system for advanced metering infrastructure in smart grid: A feasibility study." IEEE Systems Journal 9(1):31–44.

[55] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam. (2011) "Distributed intrusion-detection system in a multi-layer network architecture of smart-grids." IEEE Transactions on Smart-Grid 2(4):796–808.

[56] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani. (2009) "A detailed-analysis of the KDD CUP 99 data set. " IEEE Symposium on Computational-Intelligence for Security and Defense-Applications (CISDA) 1–6.

[57] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali. (2015) "Smart-grid cyber security: Challenges and solutions," International Conference on Smart-Grid and Clean Energy Technologies (ICSGCE) 170–175.

[58] D. Kushner. (2013) "The real story of stuxnet." IEEE Spectrum 50(3):48–53.

[59] M. Erol-Kantarci, H. T. Mouftah. (2013) "Smart grid forensic science: applications, challenges, and open issues." IEEE Communications Magazine 51(1):68–74.