electronics

MDPI

Review

Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control

Lipi Chhaya [1,*], Paawan Sharma [1], Govind Bhagwatikar [2] and Adesh Kumar [1]

[1] Department of Electronics, Instrumentation and Control Engineering, University of Petroleum & Energy Studies, Dehradun, 248007, India; PAAWAN.SHARMA@ddn.upes.ac.in (P.S.); ADESHKUMAR@ddn.upes.ac.in (A.K.)

[2] Wind & Solar Energy, SANY Group, Pune, 410501, India; gowind.india@gmail.com

* Correspondence: lipi.chhaya@gmail.com; Tel.: +91-991-337-9801

Academic Editor: Alfredo Vaccaro

Received: 21 October 2016; Accepted: 23 December 2016; Published: date

Abstract: The existing power grid is going through a massive transformation. Smart grid technology is a radical approach for improvisation in prevailing power grid. Integration of electrical and communication infrastructure is inevitable for the deployment of Smart grid network. Smart grid technology is characterized by full duplex communication, automatic metering infrastructure, renewable energy integration, distribution automation and complete monitoring and control of entire power grid. Wireless sensor networks (WSNs) are small micro electrical mechanical systems that are deployed to collect and communicate the data from surroundings. WSNs can be used for monitoring and control of smart grid assets. Security of wireless sensor based communication network is a major concern for researchers and developers. The limited processing capabilities of wireless sensor networks make them more vulnerable to cyber-attacks. The countermeasures against cyber-attacks must be less complex with an ability to offer confidentiality, data readiness and integrity. The address oriented design and development approach for usual communication network requires a paradigm shift to design data oriented WSN architecture. WSN security is an inevitable part of smart grid cyber security. This paper is expected to serve as a comprehensive assessment and analysis of communication standards, cyber security issues and solutions for WSN based smart grid infrastructure.

Keywords: communication standards; cyber security; intrusion detection system; smart grid; topology control; wireless sensor networks

1. Introduction

The electrical grid is being revolutionarily transformed as Smart grid. Smart Grid is an automated and broadly distributed energy generation, transmission and distribution network. It is characterized by full duplex network with bidirectional flow of electricity and information. It is a close loop system for monitoring and response [1–4]. Smart Grid is being conceptualized and developed by various organizations around the world such as National Institute of Standards and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), European Technology Platform (ETP), International Electrotechnical Commission (IEC), Electric Power Research Institute (EPRI), etc. Diverse set of standards and harmonization between various standards are also being rigorously researched by these organizations [4]. It can be defined in various ways as per its functional, technological or beneficial aspects. As per the definition given by U.S. department of energy, "A smart grid uses digital technology to improve reliability, security, and efficiency (both economic and energy) of the electric system from large generation, through the delivery systems to

electricity consumers and a growing number of distributed-generation and storage resources" [5]. Smart Grid is an integration of electrical as well as information and communication technologies to make the power grid more reliable, flexible, efficient and robust. It is an intelligent power grid with assimilation of various alternative and renewable energy resources. Automated monitoring, data acquisition, control and emerging communication technologies are the most prominent features of smart grid deployment. Use of diverse set of communication standards requires analysis and optimization depending upon constraints and requirements [6–9]. These requirements can be decided on the basis of area of coverage, type of application, bandwidth requirement, etc [10]. Smart grid hierarchical communication network can be categorized as Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN) as per the applications of communication technologies at various levels of deployment of smart grid [10].

1.1. Home Area Network

HAN is applicable for home automation. It is used for the consumer domain and consists of electronics appliances and wireless sensor networks [8–11]. These consumer electronics appliances communicate their energy consumption statistics to central home monitor and regulator or smart meter. Central regulator or smart meter sends it to the central electricity grid for monitoring, control, fault detection and billing purposes. Smart meters and intelligent electronic devices receive the commands from central power grid and they control the home appliances based on the received commands. Home Area Networks (HANs) have the coverage area of few meters. IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee), IEEE 802.11 (WLAN/Wi-Fi), IEEE 802.3 (Ethernet), Narrowband PLC (Power line communication), etc. standards can be used for Home area networks [10–16].

1.2. Neighborhood Area Network

The function of Neighborhood Area Network (NAN) is to communicate the information collected by smart meters to central controller [8]. The NANs may contain few hundreds of smart meters deployed in HANs. Smart meters are linked with different gateways through NANs. The coverage region of NANs is around 1–10 square miles. The requirement of data rates for NAN is around 10–1000 Kbps [11–14].

1.3. Wide Area Network

The Wide Area Network (WAN) connects various NANs. Data collection points are located at various places and the collected data are forwarded to central controller. The coverage area for WAN is around thousands of square miles [13–16]. The requirement of data rate is around 10–100 Mbps. Wide area network requires very high bandwidth for its operation and management. WAN is suitable for Supervisory Control And Data Acquisition (SCADA) systems for monitoring, data acquisition, control and management of power grid [14–17]. With the advancement in communication standards and embedded systems, wireless sensor networks have become an inevitable component of smart grid technology. They can be used to bring intelligence in power grid due to their capability to collect, store, process and communicate information [18–23]. The layered architecture of Smart Grid in terms of national, continental and intercontinental power management is also crucial for design and deployment of interconnected networks [24].

At present, Smart Grid is the most inventive technology being explored by researchers over the world. Design and testing of communication network for Smart Grid layered architecture using Zigbee technology is discussed in [24]. Other technologies such as Wi-Fi, Wimax and Bluetooth are considered for Smart Grid communications in [22–28]. Implementation of Internet of Things (IoT) for Smart Grid is explored in [29]. Recent progress in advanced metering is depicted in [30].

Cyber security for Smart Grid infrastructure is an inevitable requirement for reliable operation of utilities. Cyber security threats and solutions for smart grid are analyzed in various studies [31–38. A critical case study on overall Smart Grid security aspects and solutions for HAN based on Zigbee technology is described by Saponara et al. [39]. The authors have depcted the lessons learnt

from implementation of smart microgrid using personal area network based on IEEE 802.15.4 standard in University of Pisa in [39]. The relation between intricacy and security has been pointed out by Schumacher et al.: "Complexity is the worst enemy of security" [40] (p. 531). The technologies and policies for alternative fuels and vehicles are discussed in [41] and [42].

Smart Grid is an interconnected, hierarchical and heterogeneous network with enormous complexities and dynamics. Thus, gigantic network architecture of Smart Grid creates many security challenges. However, the above-mentioned statement is divergent for WSN as it contains tiny sensor nodes with limited computational and storage capabilities. For WSN, simplicity of design and implementation becomes the worst enemy of its security and makes it more vulnerable to attacks.

WSN is an essential component of Smart Grid communication infrastructure. Overall cyber security concerns and solutions for Smart Grid network are widely described in literature. Attacks, vulnerabilities and Security requirements for WSN are different from the overall network security essentials due to design and limitations of sensor nodes. The address specific security attacks and solutions may not be applicable for data oriented approach of WSN as communication between sensor nodes is concerned with the data rather than the address of a specific sensor node. For example, readings of humidity and temperature of a specific area can be sent by redundant nodes. Thus, the security of redundant sensor nodes should also be considered. Security of WSN is one of the most vulnerable, complicated and challenging aspects of Smart Grid security. It can be considered as a base of entire Smart Grid network security. This paper is focused on WSN attacks, detection methodologies and security aspects. It is expected to serve as a reference for design of secured sensor network for Smart Grid applications. Authors of this paper have described a layered communication architecture of Smart Grid, importance and complexities of WSN security as well as topology control methods for state of the art readers.

2. Application of Wireless Sensor Networks in Smart Grid

WSN is a cost effective solution for monitoring, control, measurement and fault diagnosis in various domains of smart grid network. A sensor node mainly contains sensors, memory, processor, power supply, transceiver and actuator. Sensors are used to sense various quantities like humidity, temperature, current, etc. Generally, WSN nodes are battery powered. Figure 1 shows the basic structure of WSN node.

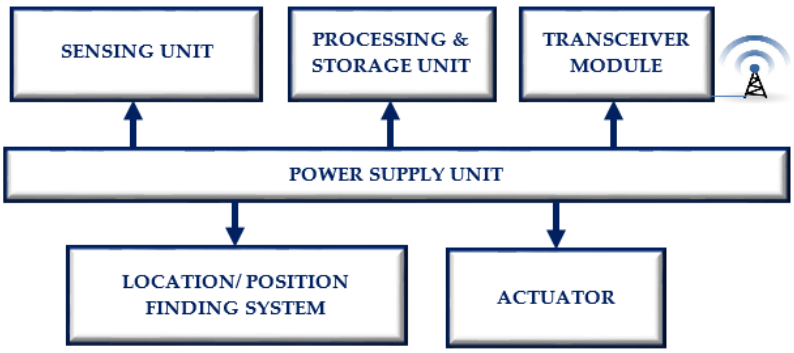

Figure 1. Architecture of WSN (Wireless Sensor Network) node.

WSN facilitates both sensing and communication requirements [21–23]. Small sensor nodes collectively form a sensor network which is used for remote wireless communication in HAN, NAN and WAN [21]. Large scale deployment of sensor nodes can be used to communicate the conditions of various generation, transmission and distribution units. Wireless sensor nodes can provide economical solution for smart microgrid monitoring which facilitates high penetration of renewable energy sources. WSN is a significant part of advanced metering infrastructure (AMI). Sensing and communication are crucial for Plug in Hybrid Electric Vehicle (PHEV) system which is one of the most ingenious component of smart grid technology. PHEV contains gasoline or diesel engine with an electric motor as well as a large rechargeable battery. PHEV can be recharged from an electrical

power outlet. It has the potential to reduce Green House Gases (GHG) emissions and carbon footprint [38–40]. PHEV facilitates flexibility as well as economy in fuel usage [41–43]. WSN can be used to communicate PHEV statistics to upstream network layers for operation and control of Smart Grid components. This information will be online available to various stakeholders through a web of sensor nodes [44–48]. An effective remote monitoring, diagnosis and control can prevent cascaded disastrous events and breakdowns [49–51]. Wireless sensor networks can be used for accurate monitoring of generation, transmission, distribution and consumption of electricity [52–55].

WSN is the most suitable solution for HAN, NAN, WAN and smart microgrid applications for integration and operation of renewable energy sources [54–59]. Figure 2 shows the application of WSN at different levels of smart grid.

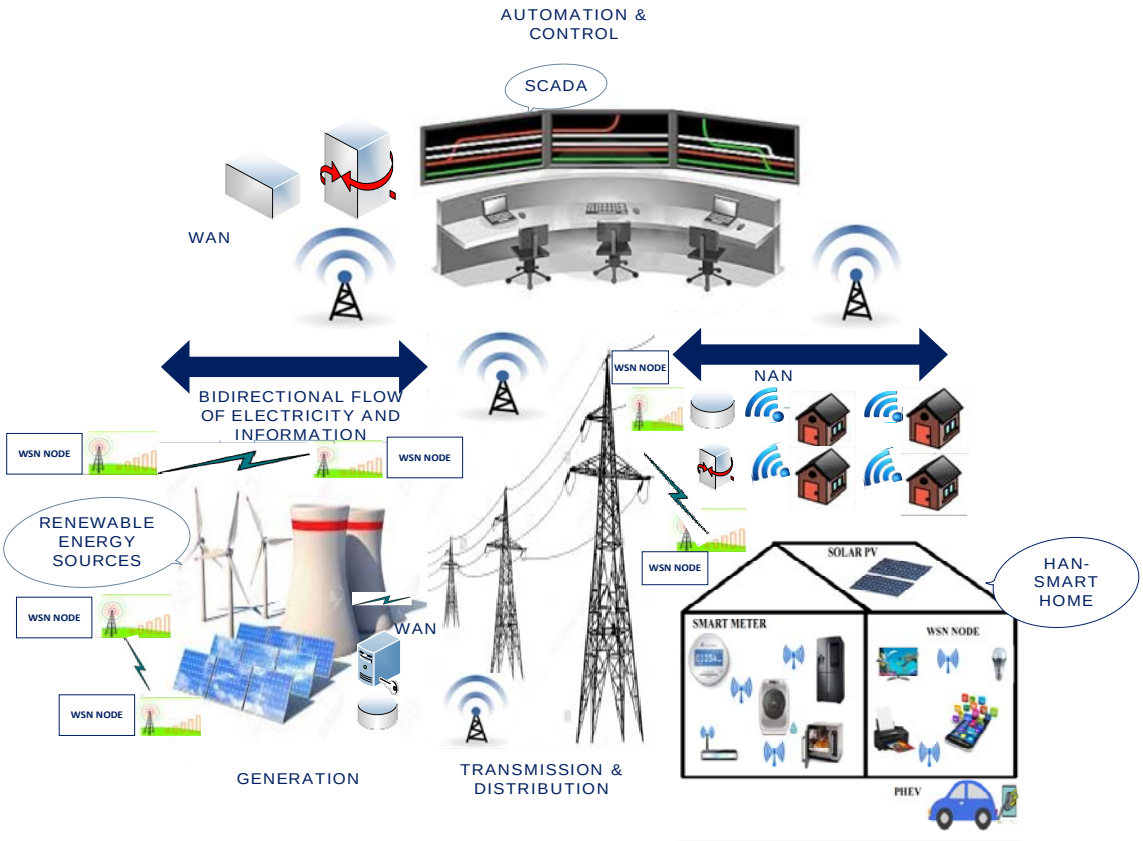

Figure 2. Application of WSN in smart grid hierarchical architecture.

Wireless sensor networks are applicable for the following smart grid utilities:

- Smart power generation

Wireless sensor networks can be used at the generation side for monitoring and management of produced energy. It is a prominent solution for smart microgrid applications using renewable energy resources. WSN can be used in solar farm, wind farm, biogas plant, etc. to monitor and control intermittent energy. One of the objectives of smart grid is to expedite the use of renewable energy sources. Renewable energy resources are situated in harsh environments and hostile locations. Moreover, their unpredictable behavior creates more challenges during their operation and management. WSN nodes are economical solutions for monitoring the behavior of renewable energy resources [55–58]. Various parameters of generating equipment can be effectively measured, communicated and controlled using WSN.

- Smart power transmission and distribution

Transmission and distribution of power contains various components like overhead transmission lines, underground cable network, substations and distribution transformers. WSN is an essential element of SCADA system. Real time remote monitoring of these components is

inevitable to prevent power failures due to equipment breakdown or malicious attacks. Wireless sensor networks can be used for power monitoring, fault detection and isolation, location discovery and outage detection [56–59].

- Customer applications

Wireless sensor network is an effective and prominent solution for home automation systems. It can be used for complete energy management of customer premises. Consumer plays an active role in smart grid technology. Consumers have the power to decide the time of use and rates of energy usage in smart homes [56–59]. For these applications, wireless sensor networks are inevitable for communication and processing of information. WSN is the backbone of smart home applications and HAN [57].

3. Challenges of Wireless Sensor Networks in Smart Grid Applications

WSNs are a vital part of self-healing smart grid network as sensor nodes communicate parameters pertaining to conditions of various equipment and energy sources. However, there are many challenges in deployment and operation of WSN due to limitations of sensor nodes and complexity of heterogeneous smart grid network [53–58]. The challenges are summarized in Table 1.

Table 1. Challenges of WSN.

Major Challenges	Description
Severe ecological conditions	Wireless sensor nodes can be subjected to harsh environmental condition which may cause fault in wireless sensor node.
Various network topologies	Heterogeneous network topologies in energy distribution network due to various features and failure of sensor nodes may cause technical challenges in design of sensor nodes.
Limited capability	Restricted processing and memory capabilities cause various challenges in design and deployment of wireless sensor networks.
Bit errors	In communication systems, high bit error rates are observed due to high noise level. This calls for various error detection and correction schemes. Detection and correction of errors require greater memory and processing facilities which make the design of sensor network challenging.
Security of sensor networks	Security of wireless sensor network is an indispensable and decisive requirement. The sensor nodes must be secured from physical tampering to hacking for smooth functioning of various smart grid applications. Physical tampering is also called node capture.
Quality of service necessities for smart grid environment	The parameters like high data rates, latency, reliability and authenticity are vital for quality of service necessities of smart grid applications. Wireless sensor networks must fulfill these criterions for successful implementation of various applications.

4. Communication Standards for Wireless Sensor Networks

The address oriented traditional communication network is based on dedicated physical and network identification of transmitter and receiver. As WSNs include redundant nodes to compensate for degraded signal strengths of the nodes or node failure, in a WSN, the specific address of a node is of least concern. Measured values must be communicated between nodes irrespective of an address of the node. Thus, WSN communication is data oriented. WSN communication architecture design entails a conceptual paradigm shift based on applications. The communication standards applicable for WSN are described as below.

4.1. Zigbee

Zigbee is based on IEEE 802.15.4 standard. It is an energy proficient short range wireless communication technology. It functions in the ISM (Industrial, scientific and medical) band which is allocated for industrial, scientific and medical applications. Zigbee operates in the band of 2.4 GHz, 868 and 928 MHz with full duplex wireless data transmission. IEEE 802.15.4 standard describes physical layer and media access layer and Zigbee Alliance has expanded the configuration of an application layer and network layer. The maximum throughput achievable by Zigbee is 250 Kbps [51]. In the area of power automation, it is applicable for smart meters, power system monitoring and measurement of various electric parameters. Smart Grid integrates information and communication technology with an existing power system to improve the power grid network with the capabilities of self-healing, disaster recovery, interoperability, compatibility, energy efficiency and security [52–55]. Zigbee can play an imperative role in operation and maintenance of power grid, data accumulation, parameter measurement, security, monitoring and consumer interface [59].

4.2. Bluetooth

Bluetooth is a short distance wireless communication technology based on IEEE 802.15.1 standard. It uses short wavelength wireless transmission in the unlicensed ISM band from 2400 to 2480 MHz. It uses frequency hopping spread spectrum (FHSS) technology and around 1600 hops per second. Its key features are extensive availability, low power consumption and rapid data exchange. Bluetooth was initially developed in 1994 by Ericsson and then a group of firms formed a special interest group to retain and improve this technology. There are two network topologies used in Bluetooth which are termed as Piconet and Scatternet. A Piconet is created by a Personal Area Network in which one wireless client acts as a master and other wireless clients serve as slaves. Maximum eight devices can communicate with each other in one Piconet. A Scatternet is an arrangement of group of Piconets. Bluetooth is used for communications between smart consumer appliances, energy management system and smart meters. It has peak data throughput of 1 Mbps, 79 radio frequency channels and channel bandwidth of 1 MHz. It has nominal range of around 10 m. Bluetooth comprises of three power classes each having a different range [59].

4.3. Wireless Fidelity or Wireless local area network

Wireless Fidelity (Wi-Fi) or wireless local area network technology is established on the basis of IEEE 802.11 standard. Wireless local area networks are prevalent for LAN applications with peak data rates of around 150 Mbps and extreme coverage range of 250 m. Wi-Fi (IEEE 802.11b) operating on 2.4 GHz band achieves maximum data rates of 11 Mbps. Other versions based on IEEE 802.11a standard operates in 5.8 GHz band using Orthogonal Frequency Division Multiplexing (OFDM) and IEEE 802.11g (improved version of Wi-Fi) operating on 2.4 GHz band provides data rate up to 54 Mbps. IEEE 802.11 provides data rates of up to 600 Mbps using Multiple Input-Multiple Output (MIMO) technology. Security concerns for Wireless local area networks are addressed and solved in IEEE 802.11i standard using Wi-Fi Protected Access (WPA-2) encryption. It uses an Advanced Encryption Standard (AES). The main feature of Wi-Fi is existing wide support in most of the electronic devices. It is an upper layer protocol which allows communication over an Internet without using a protocol translator. Restricted number of channels can be used without an overlap in Wi-Fi/WLAN. This means that a restricted number of wireless clients can be connected in a Network. However, advantages of Wi-Fi are high data throughput, wide spread availability, IP support and network scalability. A self-healing network for HAN applications with the combination of WLAN and wireless mesh network can be developed [54–58].

4.4. Z-Wave

Z-Wave protocol is specifically designed for smart home applications. It can be adopted in Home area networks of smart grid. Z-Wave is a low data rate, short range radio frequency mesh networking standard operating on 908 MHz band. The maximum coverage area is 30 m indoor and

100 m outdoor. It does not require central coordinator but employs master and slave nodes. It can support 232 devices. The data rate is from 9.6 Kbps to 40 Kbps [59].

4.5. WirelessHART

WirelessHART protocol is designed for industrial automation. It is a real-time, centralized and multi-hop mesh network developed for industrial monitoring and control applications [60–62]. It is based on IEEE 802.15.4 compatible radio and operates on 2.4 GHz ISM band. It uses direct sequence spread spectrum (DSSS) technology. Besides DSSS, it uses Time Division Multiple Access (TDMA) technology in which 10 ms time slots are allocated to nodes. The range of this technology is up to 200 m. Security of communications is maintained using 128 bit AES encryption [62]. Individual session keys as well as common network encryption keys are shared among all nodes for broadcast services. WirelessHART overcomes all the shortfalls of Zigbee in terms of robustness, reliability, security and message delivery [60–64].

4.6. 6LoWPAN

6LoWPAN is suitable for home automation system for smart homes. It is based on an integration of IPv6 and IEEE 802.15.4 standards. It is a Low Power Wireless Personal Area Network. It can be used in HAN for various applications such as smart metering, control of home appliances, sensing and automation as well as Internet of Things (IoT). It is based on 2.4 GHz band and sub-1 GHz band. It uses AES-128 encryption technique. It provides 20–250 Kbps data rates in the range of 10 m to 100 m [59].

4.7. Wavenis

Wavenis is an emergent wireless communication technology for low power machine to machine communication applications. It can be used for distances up to 200 m for various indoor applications. This technology can be used in various metering applications in smart grid. It can be used in automatic meter reading, advanced metering infrastructure and remote communication applications. Wavenis operates in the bands of 868 MHz, 915 MHz, and 433 MHz. The data throughput of Wavenis ranges from 4.8 Kbps to 100 Kbps [59]. Table 2 shows the comparative analysis of various communication standards for WSN.

Wireless sensor network (WSN) uses various short distance communication technologies as they are suitable for power efficiency and wide spread availability. These communication standards use unlicensed ISM band for their operation which makes WSN effective for communication but vulnerable to attacks.

Table 2. Comparative analysis of various communication standards for WSN (Wireless Sensor Network).

Protocol/Standard	Spectrum Type	Frequency Band	Maximum Data Throughput	Coverage Range	Advantages	Disadvantages	Market Espousal
Zigbee	Unlicensed	868 MHz, 915 MHz, 2.4 MHz	250 Kbps	Up to 100 m	Low cost, Low power usage, Less complex	Low data rate, Short range, Interference with other technologies using ISM band, Low battery power supply	Very High
Bluetooth	Unlicensed	2.4 GHz	21 Kbps	Up to 100 m	Low power usage	Low data rates, Very short range, Less secured, Interference with other technologies using ISM band	Very High
Wi-Fi	Unlicensed	2.4 GHz, 5.8 GHz	2 Mbps to 54 Mbps	Up to 250 m	High data rates, Robust, Point to point and point to multipoint communication, Low cost, IP support and network scalability	Complex design, Prone to interference, data rates may deteriorate due to interference or co-existence problems	Very high
Z-Wave	Unlicensed	868 MHz, 908 MHz	9.6 Kbps to 40 Kbps	Up to 30 m	Low power usage	Very Low data rates, Short range	Medium
WirelessHART	Unlicensed	2.4 GHz	Up to 250 Kbps	200 m	Simple and low cost solutions, Allows co-existence of multiple networks, Keeps the black and white list of devices, Self-organizing standard, More secured	All the devices operating on WirelessHART must have routing capability, No directive on how the network is configured by network manager	Very high for industrial control applications
6LoWPAN	Unlicensed	868 MHz, 915 MHz, 2.4 MHz	Up to 250 Kbps	Up to 100 m	Low power usage	Low data rates, Short range	Medium
Wavenis	Unlicensed	868 MHz, 915 MHz, and 433 MHz	4.8 Kbps to 100 Kbps	Up to 200 m	Low power usage	Very Low data rates, Short range	Very low

5. Security Issues and Cyber Attacks in Wireless Sensor Networks

The wireless sensor networks used for smart grid applications have different characteristics than communication networks used for other generic applications. These characteristics are in terms of deployment topology, data processing, environmental conditions and network throughput. The security issues are related to confidentiality, authentication, availability, integrity, authorization and newness. Confidentiality deals with secrecy of data communication. Authentication is necessary for prevention of fake messages from malicious sensor nodes. It ensures data authenticity. Availability means consistency in services in presence of attacks. Integrity means the data or messages are received in an unaffected form at the destination. Authorization means only authorized sensor nodes can communicate and unauthorized access of data must be prevented. Newness of data is inevitable to ensure that attackers do not replay the old data again to hinder the security of WSN [65–67]. It is very challenging to ensure the stated measures of data authenticity and security in WSN due to following constraints mentioned in Figure 3.

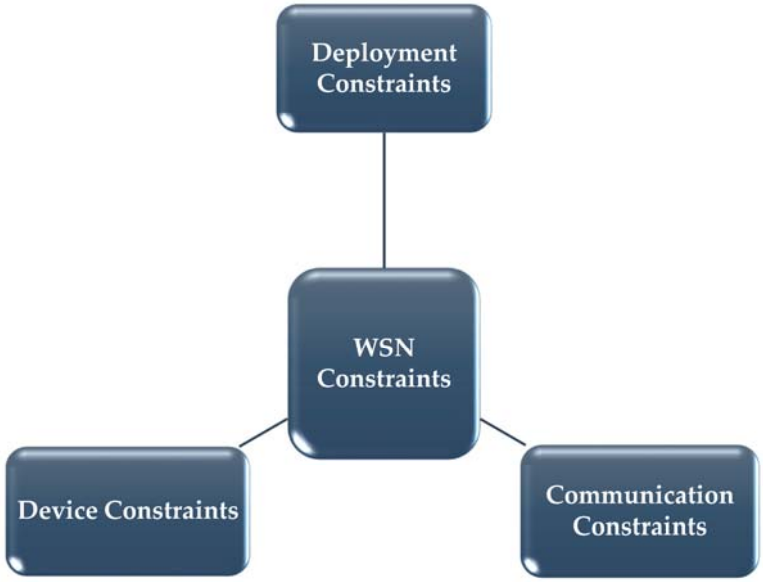

Figure 3. Major WSN constraints.

- Device Constraints: WSN nodes have very limited storage, processing and computational capabilities. They have limited power as they are battery operated.
- Deployment Constraints: Sensor nodes are deployed in potentially unsecured environments. They are deployed either in fixed manner or in random manner. They are remotely managed and controlled [66–69].
- Communication Constraints: WSNs communicate using radio transmissions and most of them use unlicensed ISM band which is used for many other applications. Co-existence of various wireless standards is a major challenge for secured communication.

Due to above reasons, sensor nodes are prone to eavesdropping or jamming attacks. Moreover, limited processing and storage capabilities of sensor nodes prevent the use of advanced cryptographic methods. Public key cryptography requires expensive computational techniques. Limited batteries of WSN make them prone to denial of service attacks which can further drain the energy from sensor nodes. Tampering of sensor nodes and reprogramming of chip are the possible attacks. The security of WSN can be endangered by reverse engineering [65–68]. Smart grid also employs various devices and communication protocols at different network levels. Thus, WSN interoperability and security with other devices is also a matter of concern. The protection and privacy of WSN must be treated carefully for smart grid applications which is a broad network comprising of enormous networks and protocols. The public and private security measures for WSN in various smart grid applications require costly solutions [67–69]. The cost–security tradeoff must

be carefully implemented. Figure 4 shows the complete overview of applications, security issues and objectives of WSN for smart grid network.

Figure 4. An overview of applications, security issues and security measures for WSN based smart grid architecture.

In addition to above wireless network security issues, WSNs are vulnerable to cyber-attacks on various network layers [70]. Figure 5 depicts the classification of various cyber-attacks in WSN.

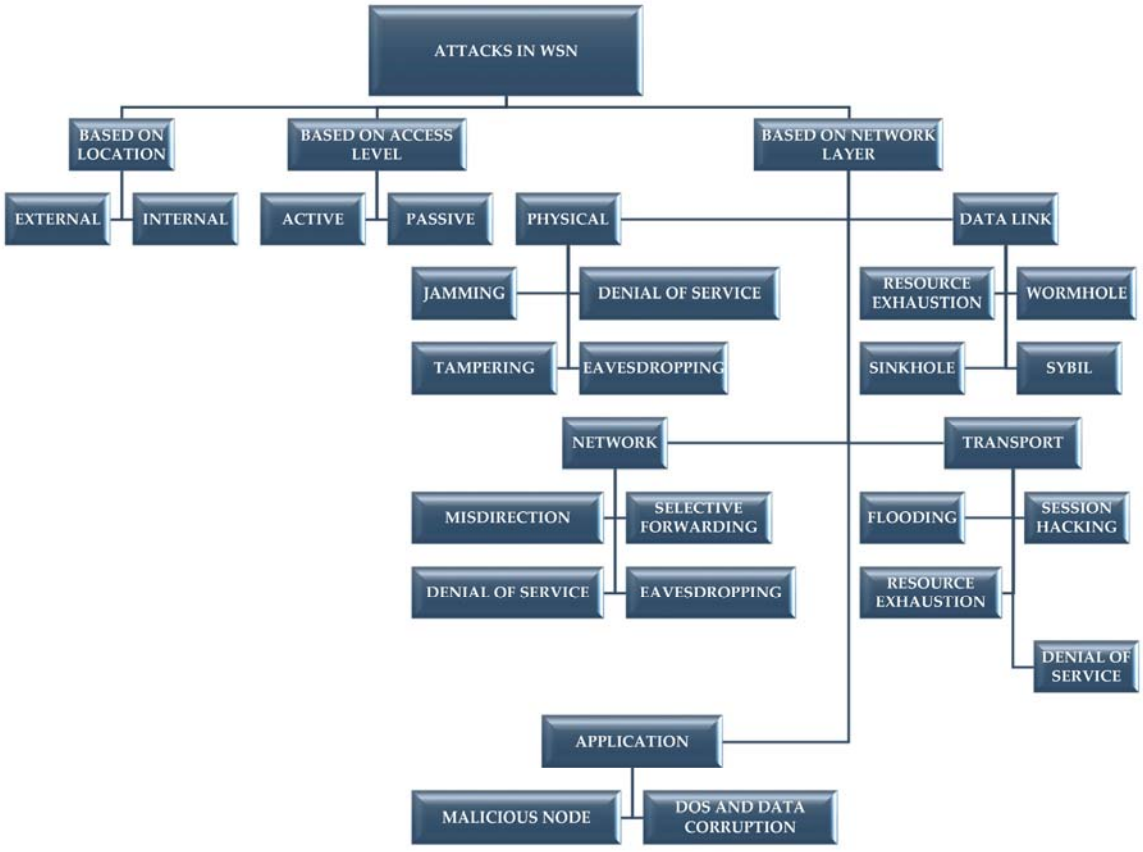

Figure 5. Classification of various attacks in WSN.

5.1. Attacks Based on Location of an Intruder

5.1.1. External Attack

Most cyber-attacks are external in nature, where an intruder is outside the range of WSN. External attacks are performed by jamming the network, exhausting the resources or denial of service (DOS) [71–75].

5.1.2. Internal Attack

In this type of attack, an intruder is in the range of WSN. This type of attack is performed by physical tampering of node, revelation of confidential information, causing denial of service to authorized node etc. [71–75].

5.2. Attack Based on Access Level of an Intruder

5.2.1. Active

This type of attack is performed by an adversary through modification and theft of data. In active attacks, an attacker performs some operation in order to hamper the confidentiality, availability and integrity of data. An adversary performs the attack by packet modification, false data injection, resource exhaustion and node capturing. Spoofing, jamming, wormhole, hello flood, DOS, sink hole, etc. are the examples of active attacks [72–76].

5.2.2. Passive

Passive attacks are performed by an intruder mainly through an observation of network activities [75]. This type of attack impedes confidentiality of the network. This type of attack includes analysis of traffic, decryption of vulnerable data, capture of information, etc.

5.3. Attacks on Various Network Layers

5.3.1. Denial of Service Attack

Restricted memory and less computational capacity of wireless sensor network make them vulnerable of denial of service attack [71–80]. In this attack, network resources are made inaccessible by network congestion [70–73].

Three types of denial of service attacks are described in the literature [70–74].

- Physical devastation/Node capture of wireless sensor nodes

Wireless sensor nodes are deployed and distributed at various places for various applications and there are possibilities of physical damage or destruction of nodes by attackers. Node capturing may result into alteration of hardware and software of WSN node [75–77].

- Utilization of network resources by intruders and making the scarce resources unavailable

Attackers or intruders can exploit the limited network resources and make them unavailable for actual users.

- Alteration of configurations of wireless sensor network by attackers

The encryption and other WSN configuration aspects must be confidential and any alterations made by intruders make them unapproachable for genuine users. Jamming of network, camouflaging the wireless sensor network ambiance and physical attack on sensor nodes are common threats.

5.3.2. Misdirection Attack

In the misdirection attack, the information is routed towards fake path. It alters the routing information of network and affects the communication adversely. Misdirection is a network layer attack. Authentication techniques between transmitter and receiver, multi hop routing, etc. can be used to detect misdirection attack.

5.3.3. Selective Forwarding

Selective forwarding is a network layer attack. In this type of attack, a counterfeit node acts like an actual node and divert the packets to a wrong path but selectively drops some of the packets so

that it becomes difficult to identify the intrusion. Acknowledgement based routing, multi data flow and detection based on neighboring information can be used to detect this type of intrusion [70–75].

5.3.4. Sink Hole Attack

Sink hole attack is a data link layer attack. In this attack, an intruder comes with an agreement with a sensor node or introduces a fake node in the sensor network. When a forged node attracts the network traffic, an attack is generated. Once the attack is successful, the forged node can perform various malfunctions like dropping all packets, dropping selective packets and alteration of data [70–76].

5.3.5. Sybil Attack

In Sybil attack, a malicious sensor node takes multiple identities to perform an attack. In wireless sensor network, all the sensor nodes work complaisantly but this type of attack targets this cooperation and disturbs the routing and communication process [76–83].

5.3.6. Wormhole Attack

Wormhole attack is a data link layer intrusion. In this type of attack, a malicious or fake node registers all the information and diverts it to wrong path. This attack can be formed without the knowledge of cryptography of actual wireless sensor node [84–86].

5.3.7. Hello Flood Attack

In wireless sensor networks, routing protocols use Hello packets for detection of neighbors. In this type of attack, fake packets are used to camouflage hello packets and to attract the sensor nodes [70]. Attackers with ample radio resources and processing capabilities can generate this type of attack. The victim node will identify false hello packet as normal node.

Various cyber-attacks concerning different network layers and their respective countermeasures are described in Table 3.

Table 3. Various cyber-attacks in WSN and their countermeasures.

Layer	Attack	Countermeasures
Physical	DOS (denial of service), Jamming, Node Capture	Spread spectrum technology, Adaptive antennas
Data Link	Wormhole, Sink hole, Sybil, Resource exhaustion	Link layer cryptography
Network	DOS, Misdirection, Selective forwarding, Eavesdropping	Key management, Secured routing, Topology control
Transport	Flooding, Session hacking, Resource exhaustion, DOS	Intrusion detection, encryption
Application	DOS, Data corruption, Malicious node	Intrusion detection, Malicious node isolation

6. Intrusion Detection System

Encryption and authentication are unavoidable considerations for the security of any communication system. These parameters are vital for reliability, confidentiality and integrity of sensor network. Detection of attack or intrusion is also imperative to make the system robust against attacks. Intrusion detection system (IDS) can be termed as a subsequent security measure and defense mechanism against cyber-attacks [82]. IDS observes the network and identifies anomalous activities. IDS can be defined as a unification of hardware and software tools which are meant to detect internal or external cyber-attacks. IDS is essential for fault tolerance, security and reliability of WSN. IDS also investigates the physical tampering of sensor node. This ensures secured routing of information over WSN. The principle tasks of IDS are prevention and detection of attacks, situational awareness, evidence collection, and administration of connection topologies [77–83]. Security of WSN is more complex compared to Mobile and Adhoc Networks (MANETs) due to

resource constraints in WSN [83]. This calls for an efficient IDS for secured WSN communication. The main components of IDS are as follows.

- Sensor: It collects statistics from the system being monitored.
- Detector: It analyzes collected data to identify intrusions.
- Information Base: It supports the detector by providing attack signatures.
- Response Manager: It manages the responses to the cyber-attacks.

The general block diagram of IDS is shown in Figure 6.

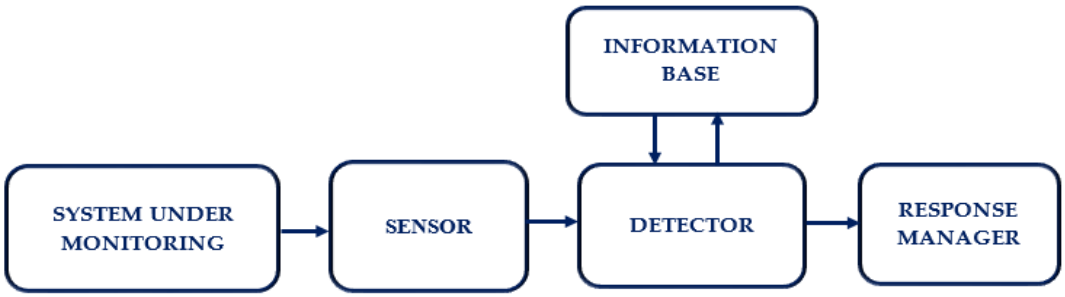

Figure 6. General block diagram of intrusion detection system.

The strategies for attacks and detection system for WSNs are different from other wireless or wired networks due to their structure and limited battery life. Intrusion detection approaches for WSN are classified as follows [82–86].

6.1. Anomaly Detection

Different types of anomalies of WSN are node anomaly, network anomaly and data anomaly as described below.

- Node Anomaly: This types of anomalies can be detected during failure of WSN node or power problems. Failure of solar panel, or fluctuations in power of different components can cause this type of anomaly. Node anomalies can be due to hardware or software issues in the WSN nodes [82].
- Network Anomaly: Unexpected fluctuations in the signal strength and connection problems can be used to detect network anomaly. Complete loss of connectivity or episodic connectivity can be used to detect intrusions in the network.
- Data Anomaly: An intrusion attempt can be detected from chaotic or disordered data communication.

Detection of a specific type of anomaly is very useful to decide the type and explication of cyber-attack. To detect the above-mentioned anomalies, different types of approaches are applied [86]. These anomaly detection approaches can be classified as game theoretic, statistical, machine learning, artificial immune system and data mining based approach [85–88].

6.2. Misuse Detection

Misuse detection is a signature based intrusion detection system to discover recognized attacks. The limitation of this type of detection system is that it cannot detect unknown attacks which are not predefined. Moreover, keeping signatures of attacks to generate data base is a complicated task for WSN due to its limited memory and processing capabilities. However, in very few studies, this method has been explored using watchdog approach [83–86]. Watchdog approach uses the abnormal behavior of a node to detect an intrusion. All nodes watch the performance of their neighbors and communicate the information about their behavior.

6.3. Hybrid Detection

An intrusion detection approach that does not qualify to be classified as either anomaly or misuse detection is called hybrid detection method. This approach is application specific and it is manually defined by an administrator. Hybrid approach can be a combination of anomaly and misuse detection approaches for accurate results [84–88].

IDS is inevitable for the security of WSN as it awakens the operators to take countermeasures against cyber-attacks. In addition to IDS, Intrusion Detection and Prevention System (IDPS) can also be developed for rapid and effective mitigation and avoidance of attacks [89]. In some instances, an intruder can be intelligent with detection avoidance competences. Moreover, range of communication, density of nodes, sensing algorithms, etc. play a crucial role in intrusion and its detection [90]. More research work is required against intelligent intrusion algorithms in order to maintain security, confidentiality and reliability of WSN.

7. Topology Control

Wireless sensor networks are the group of distributed sensor nodes which communicate various information for monitoring and control purpose. Sometimes placing WSN nodes in unsecured and hostile environments is required. Due to limited battery life and restricted processing and storage capabilities of WSN nodes, security against above mentioned attacks is the biggest challenge. WSN nodes are mandatory part of smart grid communication infrastructure. Apart from cryptographic approach, WSN can be designed in such a way that their topologies have specific connectivity properties [89]. Topology control can be a practical solution for WSN nodes with limited computational and communication capabilities [90–93]. An overview of various topology control schemes is described below.

7.1. Random Key Predistribution Scheme

This scheme is extensively recognized as an appropriate solution for secured WSN communication. There are two types of random key predistribution scheme.

7.1.1. Eschenauer-Gligor Random Key Predistribution Scheme (EG Scheme)

In EG scheme, there are n number of sensors in a keying network. This scheme uses an offline pool of keys containing Pn keys. Before deployment, each sensor is assigned Kn number of discrete keys selected from the pool of keys. Pn and Kn both are the functions of n for generality motives. Kn keys in each sensor establish sensor's key ring. After deployment, two sensors can establish secured communication link only if they have at least one key(s) in common i.e., $1 \leq s \leq Kn$. Confidentiality and authenticity are achieved with symmetric key encryption mode [94,95]. Figure 7 shows the EG scheme.

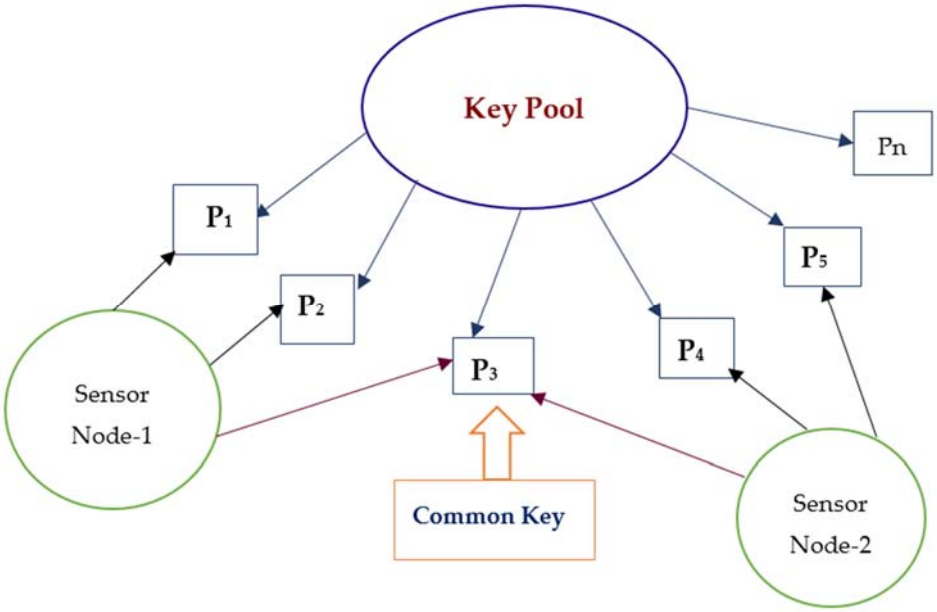

Figure 7. Eschenauer–Gligor Random Key Predistribution Scheme.

7.1.2. *s*-Composite Random Key Predistribution Scheme

s-Composite Random Key Predistribution Scheme is better than EG scheme in a manner that it requires s overlapped key in order to establish communication between two sensor nodes. It requires $s \geq 2$ for secured communication between sensor nodes. It is beneficial for small scale sensor attacks but becomes vulnerable for large scale attacks. s is selected according to desired resilience of the sensor network. Figure 8 shows the *s*-composite scheme.

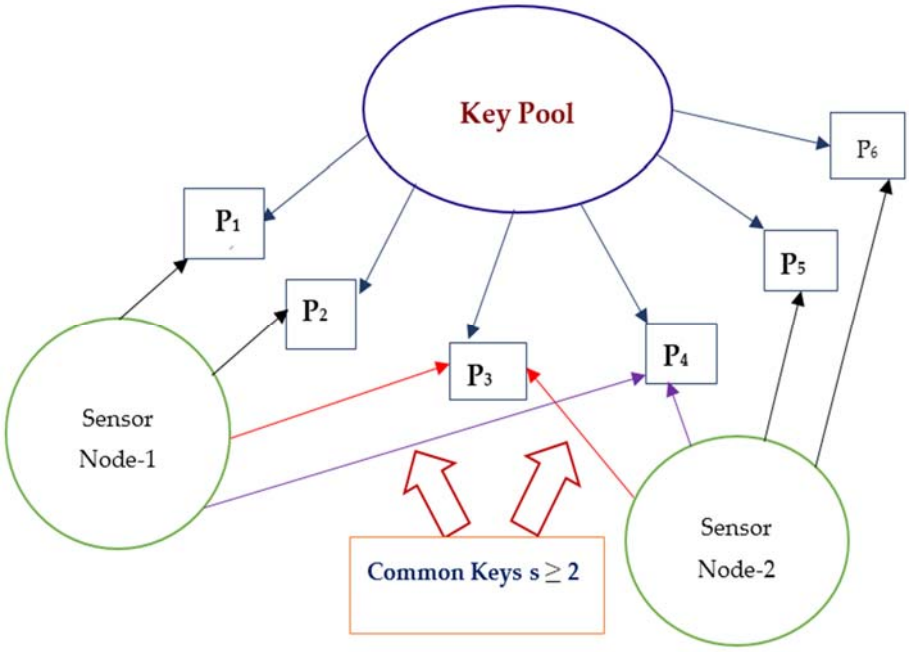

Figure 8. *s*-Composite Random Key Predistribution Scheme.

7.2. Link Constraint Models

Various link constraint models are used to explore WSN using either EG or s-composite schemes. They are classified as follows.

7.2.1. Full Visibility Model

In this model, it is assumed that there is a communication link between any two sensor nodes in a network. According to this model, the two sensors can establish a secured communication link only if they have one key for EG scheme and s keys for s-composite scheme common among them [94–97]. This model requires mutual keys between sensor nodes which satisfy both the schemes.

7.2.2. On-Off Channel Model

This model contains independent channels, each of which is either on with probability Pn or off with probability (1−Pn), where Pn is a function of n for generality. This model requires the channel between two sensors to be on for communication [96–99].

7.2.3. Disk Model

This model requires sensor nodes to be within a specific radius r_n to establish a communication link between them. For the node distribution, it is considered that all n nodes are uniformly and individually deployed in a bounded space of a Euclidean plane. Such network area A is either a torus T or a square S, each of unit area, depending on whether the boundary effect exists or not [98]. The boundary effect arises whenever part of the transmission area of a node may fall outside the network area A. T does not have the boundary effect, whereas S has the boundary effect [99–101].

8. Conclusions

The present power grid is going through a huge transformation with the deployment of smart grid technology. Smart grid is a complex hierarchical and heterogeneous network. Wireless sensor network is a prominent solution for various applications of smart grid. Wireless sensor networks are distributed collection of sensor nodes situated at various places for measurement and communication of various parameters such as temperature, voltage, current and humidity. These parameters are required for remote monitoring and control of different components of smart grid. WSNs are effective solutions for energy management system in home, industry and business applications. These small sensor nodes are extensively vulnerable to attacks as they are placed in hostile surroundings. Node capture results into complete control of attacker on the WSN node and tampering of hardware as well as software of the node. The energy exhausted sensor nodes can be easily victimized. Therefore, cryptographic security is essential to protect the communication between sensor nodes as well as to detect sensor capture and to invalidate the compromised security keys. The security of dispersed WSN nodes is a crucial technical challenge due to limited memory and computational capabilities of WSN nodes.

The data oriented design approach is required for deployment of WSN as the purpose of sensor nodes is to sense and communicate the parameters. Redundant nodes must be deployed to deal with node failures and degraded signal strengths. Traditional communication process involves physical address and IP address of a specific transmitter and receiver to establish a successful communication link. This type of communication is address oriented which is different from WSN approach. As an example, consider the measurement of average temperature of some area. In this case, temperatures from each and every node is not required but an average temperature can be calculated from received readings from sensor nodes positioned at various places. Identity of a specific node is secondary as soon as the readings from all areas are received. The challenges of WSN communication is different from the challenges faced by the usual communication networks. Rigorous and diversified research endeavors in the field of WSN security are inevitable as WSN forms the backbone of smart grid IoT applications. Moreover, various solutions for local and wide area networks are already available due to development of Internet technology. The security of gigantic network of tiny WSN networks is the most challenging aspect of smart grid reliability.

In this paper, the analysis of various wireless communication standards, cyber security issues and solutions for WSN are discussed. Nature of various attacks must be known for detection of attacks and development of different solutions at diverse network layers. Apart from well researched solutions such as IDS and cryptographic security, this paper explores topology control

for cyber security of wireless sensor networks. Various solutions for intrusion detection and prevention system must be developed for inhibition of adverse effects of cyber-attacks. Secured interoperability between various communication standards is inevitable for robust hierarchical smart grid infrastructure. WSN security is a multi-faceted research topic due to limitations imposed by communication standards and sensor nodes. The cost–security tradeoff must be critically analyzed and implemented for future applications of wireless sensor networks in smart grid applications.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
DOS	Denial Of Service
EG	Eschenauer–Gligor
ETP	European Technology Platform
HAN	Home Area Network
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
MANET	Mobile and Adhoc NETwork
MIMO	Multiple Input Multiple Output
NAN	Neighborhood Area Network
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency Division Multiplexing
PHEV	Plug in HybridElectric Vehicle
PLC	Power Line Communication
SCADA	Supervisory Control And Data Acquisition
TDMA	Time Division Multiple access
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WSN	Wireless Sensor Network

References

1. Farooq, H.; Jung, L.T. Choices available for implementing smart grid communication network. In Proceedings of the IEEE International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 3–5 June 2014; pp. 1–5.
2. Feng, Z.; Yuexia, Z. Study on smart grid communications system based on new generation wireless technology. In Proceedings of the IEEE International Conference on Electronics, Communications and Control (ICECC), Ningbo, China, 9–11 September 2011; pp. 1673–1678.
3. Fang, X.; Misra, S.; Xu, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980.
4. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38.
5. U.S. Department of Energy. Smart Grid System Report. Available online: http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf (accessed on 10 August 2016).
6. Giustina, D.D.; Rinaldi, S. Hybrid Communication Network for the Smart Grid: Validation of a Field Test Experience. *IEEE Trans. Power Deliv.* **2015**, *30*, 2492–2500.

7. Goel, N.; Agarwal, M. Smart grid networks: A state of the art review. In Proceedings of the IEEE International Conference on Signal Processing and Communication (ICSC), Noida, India, 16–18 March 2015; pp. 122–126.
8. Mulla, A.; Baviskar, S.; Khare, N.; Kazi, F. The Wireless Technologies for Smart Grid Communication: A Review. In Proceedings of the IEEE International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 4–6 April 2015; pp. 442–447.
9. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Review of communication technologies for smart homes/building applications. In Proceedings of the IEEE International Conference on Smart Grid Technologies—Asia (ISGT ASIA), Bangkok, Thailand, 3–6 November 2015.
10. Chhaya, L.; Sharma, P.; Bhagwatikar, G.; Kumar, A. Design and Implementation of Remote Wireless Monitoring and Control of Smart Power System Using Personal Area Network. *Indian J. Sci. Technol.* **2016**, *9*, 1–5.
11. Parvez, I.; Sundararajan, A.; Sarwat, A.I. Frequency band for HAN and NAN communication in Smart Grid. In Proceedings of the IEEE Computational Intelligence Applications in Smart Grid (CIASG) Symposium, Orlando, FL, USA, 9–12 December 2014.
12. Hiew, Y.K.; Aripin, N.M.; Din, N.M. Performance of cognitive smart grid communication in home area network. In Proceedings of the IEEE 2nd International Symposium on Telecommunication Technologies (ISTT), Langkawi, Malaysia, 24–26 November 2014; pp. 417–422.
13. Aalamifar, F.; Hassanein, S.; Takahara, G. Viability of powerline communication for the smart grid. In Proceedings of the 26th Biennial Symposium on Communications (QBSC), Kingston, ON, Canada, 28–29 May 2012; pp. 19–23.
14. Hartmann, T. Generating realistic Smart Grid communication topologies based on real-data. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 428–433.
15. Parikh, P.P.; Kanabar, M.G.; Sidhu, T.S. Opportunities and challenges of wireless communication technologies for smart grid applications. In Proceedings of the IEEE Power and Energy Society General Meeting, Minneapolis, MN, USA, 25–29 July 2010.
16. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 5–20.
17. Saputro, N.; Akkaya, K.; Uludag, S. A survey of routing protocols for smart grid communications. *Comput. Netw.* **2012**, *56*, 2742–2771.
18. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Trans. Ind. Inform.* **2013**, *9*, 28–42.
19. Erol-Kantarci, M.; Mouftah, H.T. Wireless multimedia sensor and actor networks for the next generation power grid. *Ad Hoc Netw.* **2011**, *9*, 542–551.
20. Binti, M.I.N.; Wei, T.C.; Yatim, A.H.M. Smart grid technology: Communications, power electronics and control system. In Proceedings of the IEEE International Conference on Sustainable Energy Engineering and Application (ICSEEA), Bandung, Indonesia, 14–15 October 2015; pp. 10–14.
21. Gungor, V.V. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539.
22. Amin, R.; Martin, J.; Zhou, X. Smart Grid communication using next generation heterogeneous wireless networks. In Proceedings of the IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 229–234.
23. Bera, S.; Misra, S.; Obaidat, M.S. Energy-efficient smart metering for green smart grid communication. In Proceedings of the IEEE International Conference on Global Communications Conference (GLOBECOM), Austin, TX, USA, 8–12 December 2014; pp. 2466–2471.
24. Batista, N.C.; Melicio, R.; Mendes, V.M.F. Layered Smart Grid architecture approach and field tests by Zigbee technology. *Energy Convers. Manag. Elsevier* **2014**, *88*, 49–59.
25. Kaebisch, S.; Schmitt, A.; Winter, M.; Heuer, J. Interconnections and Communications of Electric Vehicles and Smart Grids. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 4–6 October 2010; pp. 161–166.
26. Wang, B.; Sechilariu, M.; Locment, F. Intelligent DC Microgrid with Smart Grid Communications: Control Strategy Consideration and Design. *IEEE Trans. Smart Grid* **2012**, *3*, 2148–2156.

27. Elkhorchani, H.; Idoudi, M.; Grayaa, K. Development of communication architecture for intelligent energy networks. In Proceedings of the IEEE International Conference on Electrical Engineering and Software Applications (ICEESA), Hammamet, Tunisia, 21–23 March 2013.
28. Elkhorchani, H.; Grayaa K. Smart micro Grid power with wireless communication architecture. In Proceedings of the IEEE International Conference on Electrical Sciences and Technologies in Maghreb (CISTEM), Tunis, Tunisia, 3–6 November 2014.
29. Elarabi, T.; Deep, V.; Rai, C.K. Design and simulation of state-of-art ZigBee transmitter for IoT wireless devices. In Proceedings of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Abu Dhabi, UAE, 7–10 December 2015; pp. 297–300.
30. Garcia-Hernandez, J. Recent Progress in the Implementation of AMI Projects: Standards and Communications Technologies. In Proceedings of the International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE), Prague, Czech Republic, 9–10 July 2015; pp. 251–256.
31. Line, M.B.; Tøndel, I.A.; Jaatun, M.G. Cyber security challenges in Smart Grids. In Proceedings of the International Conference on Innovative Smart Grid Technologies (ISGT), Berlin, Germany, 14–17 October 2012.
32. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Cyber Security for Smart Grid Communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010.
33. Garner, G. Designing last mile communications infrastructures for intelligent utility networks Smart Grid. In *IBM Intelligent Utility Network (IUN) Communication Services*; IBM Australia Limited, Sydney, Australia, 2010.
34. Dzung, D.; Naedele, M.; Von Hoff, T.P.; Crevatin, M. Security for Industrial Communication Systems. *IEEE Commun. Surv. Tutor.* **2005**, *93*, 1152–1177.
35. Wang, J. *Computer Network Security*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 3–24.
36. Lee, E.K.; Gerla, M.; Oh, S.Y. Physical layer security in wireless Smart Grid. *IEEE Commun. Mag.* **2012**, *50*, 46–52.
37. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371.
38. Shapsough, S.; Qatan, F.; Aburukba, R.; Aloul, F.; Al Ali, A.R. Smart Grid cyber security: Challenges and solutions. In Proceedings of the International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Offenburg, Germany, 20–23 October 2015; pp. 170–175.
39. Saponara, S.; Bacchillone, T. Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid. *Hindawi J. Comput. Netw. Commun.* **2012**, *1*, 1–19.
40. Schumacher, M.; Fernandez-Buglioni, E.; Hybertson, D.; Buschmann, F.; Sommerlad, P. *Security Patterns: Integrating Security and Systems Engineering*; John Wiley: Hoboken, NJ, USA, 2006.
41. Ahmadi, L.; Croiset, E.; Elkamel, A.; Douglas, P.L.; Unbangluang, W.; Entchev, E. Impact of PHEVs Penetration on Ontario's Electricity Grid and Environmental Considerations. *Energies* **2012**, *5*, 5019–5037.
42. Browne, D.; O'Mahony, M.; Caulfield, B. How should barriers to alternative fuels and vehicles be classified and potential policies to promote innovative technologies be evaluated? *J. Clean. Prod.* **2012**, *35*, 140–151.
43. Guerfi, A.; Dontigny, M.; Charest, P.; Petitclerc, M.; Lagacé, M.; Vijh, A.; Zaghib, K. Improved electrolytes for Li-ion batteries: Mixtures of ionic liquid and organic electrolyte with enhanced safety and electrochemical performance. *J. Power Sources* **2010**, *195*, 845–852.
44. Amjad, S.; Neelakrishnan, S.; Rudramoorthy, R. Review of design considerations and technological challenges for successful development and deployment of plug-in hybrid electric vehicles. *Renew. Sustain. Energy Rev.* **2010**, *14*, 1104–1110.
45. Delin, K.; Jackson, S.; Some, R. Sensor webs. *NASA Tech. Briefs* **1999**, *20*, 80.
46. Gibbons, P.; Karp, B.; Ke, Y.; Nath, S.; Seshan, S. Irisnet: An architecture for a worldwide sensor web. *IEEE Pervasive Comput.* **2003**, *4*, 22–33.
47. Moodley, D.; Simonis, I. A New Architecture for the Sensor Web: The Swap Framework. In Proceedings of the International Semantic Web Conference, Athens, GA, USA, 5–9 November 2006.
48. Martinez-Sandoval, R.; Garcia-Sanchez, A.-J.; Garcia-Sanchez, F.; Garcia-Haro, J.; Flynn, D. A Comprehensive WSN-Based Approach to Efficiently Manage a Smart Grid. *Sensors* **2014**, *14*, 18748–18783.
49. Chang, K.-S.; Kang, S.-M.; Park, K.-J.; Shin, S.-H.; Kim, H.; Kim, H.-S. Electric Field Energy Harvesting Powered Wireless Sensors for Smart Grid. *J. Electr. Eng. Technol.* **2012**, *7*, 75–80.

50. Kim, K.J.; Cottone, F.; Goyal, S.; Punch, J. Energy scavenging for energy efficiency in networks and applications. *Bell Labs Tech. J.* **2010**, *15*, 7–29.
51. Sallabi, F.M.; Gaouda, A.M.; El-Hag, A.H.; Salama, M.M.A. Evaluation of ZigBee Wireless Sensor Networks under High Power Disturbances. *IEEE Trans. Power Deliv.* **2011**, *29*, 13–20.
52. Monshi, M.M.; Mohammed, O.A. A study on the efficient wireless sensor networks for operation monitoring and control in smart grid applications. In Proceedings of the IEEE International Southeast Conference, Silicon Valley, CA, USA, 6–9 October 2013.
53. Gungor, V.V.; Lu, B.; Hancke, G.P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Trans. Ind. Electron*. **2010**, *57*, 3557–3564.
54. Brak, M.E.; Brak, S.E.; Essaaidi, M.; Benhaddou, D. Wireless Sensor Network applications in smart grid. In Proceedings of the IEEE International Renewable and Sustainable Energy Conference (IRSEC), Ouarzazate, Morocco, 10–13 December 2014; pp. 587–592.
55. Zhang, Y.; Li, X.; Zhang, S. Zhen, Y. Wireless sensor network in smart grid: Applications and issue. In Proceedings of the World Congress on Information and Communication Technologies (WICT), Trivandrum, India, 3 October–2 November 2012; pp. 1204–1208.
56. Erol-Kantarci, M.; Mouftah, H.T. Wireless Sensor Networks for smart grid applications. In Proceedings of the IEEE International Conference on Electronics, Communications and Photonics (SIECPC), Riyadh, Saudi Arabia, 24–26 April 2011.
57. Erol-Kantarci, M.; Mouftah, H.T. Using wireless sensor networks for energy-aware homes in smart grids. In Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Riccione, Italy, 22–25 June 2010; pp. 456–458.
58. Brak, M.E.; Essaaidi, M. Wireless sensor network in smart grid technology: Challenges and opportunities. In Proceedings of the IEEE International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse, Tunisia, 21–24 March 2012; pp. 578–583.
59. Mahmood, A.; Javaid, N.; Razzaq, S. A Review of Wireless Communications for Smart Grid. *Renew. Sustain. Rev.* **2015**, *41*, 248–260.
60. IEEE Std. 802.15.4-2006. *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*; IEEE Press: New York, NY, USA, 2006.
61. Krishnamurthy, L.; Adler, R.; Buonadonna, P.; Chhabra, J.; Flanigan, M.; Kushalnagar, N.; Nachman, L.; Yarvis, M. Design and deployment of industrial sensor networks: Experiences from a semiconductor plant and the north sea. In Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, San Diego, CA, USA, 2–4 November 2005; pp. 64–75.
62. Horvath, P.; Yampolskiy, M.; Koutsoukos, X. Efficient Evaluation of Wireless Real-Time Control Networks. *Sensors* **2015**, *15*, 4134–4153.
63. IEEE 802.15.4g-2012. *IEEE Standard for Local and Metropolitan Area Networks Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Physical Layer (PHY) Specifications for Low Data Rate, Wireless, Smart Metering Utility Networks*; IEEE Press: New York, NY, USA, 2012; pp. 1–258.
64. Han, S.; Zhu, X.; Mok, A.K.; Chen, D.; Nixon, M. Reliable and Real-Time Communication in Industrial Wireless Mesh Networks. In Proceedings of the 17th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Chicago, IL, USA, 11–14 April 2011; pp. 3–12.
65. Lu, Z.; Lu, X.; Wang, C. Review and evaluation of security threats on the communication networks in the smart grid. In Proceedings of the IEEE International Military Communications Conference, San Jose, CA, USA, 31 October–3 November 2010; pp. 1830–1835.
66. Dini, G.; Tiloca, M. On simulative analysis of attack impact in Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Emerging Technologies & Factory Automation (ETFA), Cagliari, Italy, 10–13 September 2013.
67. Radmand, P.; Talevski, A.; Petersen, S.; Carlsen, S. Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries In Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, Australia, 20–23 April 2010; pp. 949–957.
68. Mahmood, A.; Akbar, A.H. Threats in end to end commercial deployments of Wireless Sensor Networks and their cross layer solution. In Proceedings of the IEEE International Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 12–13 June 2014; pp. 15–22.

69. Neogy, S. Security management in Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK, 8–9 June 2015.
70. Can, O.; Sahingoz, O.K. A survey of intrusion detection systems in wireless sensor networks. In Proceedings of the 6th IEEE International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 27–29 May 2015.
71. Padmavathi, G.; Shanmugapriya, D. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *Int. J. Comput. Sci. Inf. Secur.* **2009**, *4*, 117–125.
72. Malik, M.Y. An outline of security in wireless sensor networks: Threats, countermeasures and implementations. *Wirel. Sens. Netw. Energy Effic. Protoc. Routing Manag.* **2011**, doi:10.4018/978-1-4666-0101-7.ch024.
73. Shukla, J. Babli kumari security threats and defense approaches in wireless sensor networks: An overview. *Int. J. Appl. Innov. Eng. Manag.* **2013**, *2*, 165–175.
74. Nguyen, H.L.; Nguyen, U.T. A study of different types of attacks on multicast in mobile ad hoc networks. *Ad Hoc Netw.* **2008**, *6*, 32–46.
75. Mohanty, P.; Panigrahi, S.; Sarma, N.; Satapathy, S.S. Security issues in wireless sensor network data gathering protocols: A survey. *J. Theor. Appl. Inf. Technol.* **2010**, *13*, 14.
76. Han, S.; Chang, E.; Gao, L.; Dillon, T. Taxonomy of Attacks on Wireless Sensor Networks. In *EC2ND2005*; Springer: London, UK, 2006; pp. 97–105.
77. Lupu, T.G. Main types of attacks in wireless sensor networks. *World Sci. Eng. Acad. Soc.* **2009**, *9*, 180–185.
78. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315.
79. Huang, E.; Scott, C.-H.; MacCallum, E.; David, E.; Du, D.-Z. *Attacks and Countermeasures in Sensor Networks: A Survey*; Springer: New York, NY, USA, 2010.
80. Walters, J.P.; Liang, Z.; Shi, W.; Chaudhary, V. Wireless Sensor Network Security: A Survey. In *Security in Distributed, Grid and Pervasive Computing*; Taylor & Francis: Oxfordshire, UK, 2006.
81. Mohammadi, S.; Atani, R.E.; Jadidoleslamy, H. A comparison of link layer attacks on wireless sensor networks. *J. Inf. Secur.* **2011**, *2*, 69–84.
82. Rajkumar; Vani, B.A.; Rajaraman, G.; Chandrakanth, H.G. Security Attacks and its Countermeasures in Wireless Sensor Networks. *Int. J. Eng. Res. Appl.* **2014**, *4*, 4–15.
83. Kavitha, T.; Sridharan, D. Security vulnerabilities in wireless sensor networks: A survey. *J. Inf. Assur. Secur.* **2010**, *5*, 31–44.
84. Ismail, B.; Salvatore, D.M.; Sankar, R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 266–282.
85. Granjal, J.; Monteiro, E.; Sá Silva, J. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312.
86. Diaz, A.; Sanchez, P. Simulation of Attacks for Security in Wireless Sensor Network. *Sensors* **2016**, *16*, 1932.
87. Zhang, L.; Zhang, H. A Survey on Security and Privacy in Emerging Sensor Networks: From Viewpoint of Close-Loop. *Sensors* **2016**, *16*, doi:10.3390/s16040443.
88. Salehian, S.; Masoumiyan, F.; Udzir, N.I. Energy-efficient intrusion detection in Wireless Sensor Network. In Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 26–28 June 2012; pp. 207–212.
89. Sun, C.-C.; Liu, C.-C.; Xie, J. Cyber-Physical System Security of a Power Grid: State-of-the-Art. *Electronics* **2016**, *5*, doi:10.3390/electronics5030040.
90. Wang, Y.; Chu, W.; Fields, S.; Heinemann, C.; Reiter, Z. Detection of Intelligent Intruders in Wireless Sensor Networks. *Future Internet* **2016**, *8*, doi:10.3390/fi8010002.
91. Chelli, K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. In Proceedings of the World Congress on Engineering (WCE), London, UK, 1–3 July 2015; pp. 519–524.
92. Zhang, Y.; Chen, W.; Liang, J.; Zheng, B.; Jiang, S. A Network Topology Control and Identity Authentication Protocol with Support for Movable Sensor Nodes. *Sensors* **2015**, *15*, 29958–29969.
93. Pietro, R.D.; Mancini, L.V.; Mei, A.; Panconesi, A.; Radhakrishnan, J. Connectivity properties of secure wireless sensor networks. In Proceedings of the ACM Workshop on Security of Ad-Hoc and Sensor Networks, Washington, DC, USA, 25–29 October 2004; pp. 53–58.

94. Pietro, R.D.; Mancini, L.V.; Mei, A.; Panconesi, A.; Radhakrishnan, J. Redoubtable sensor networks. *ACM Trans. Inf. Syst. Secur.* **2008**, *11*, 1–13.
95. Yagan, O. Performance of the Eschenauer–Gligor key distribution scheme under an on/off channel. *Trans. Inf. Theory* **2012**, *58*, 3821–3835.
96. Jutla, C.S. Encryption modes with almost free message integrity. In Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt), Innsbruck, Austria, 6–10 May 2001; pp. 529–544.
97. Komls, J.; Szemerdi, E. Limit distribution for the existence of Hamiltonian cycles in a random graph. *Discret. Math.* **1983**, *43*, 55–63.
98. Blackburn, S.; Gerke, S. Connectivity of the uniform random intersection graph. *Discret. Math.* **2009**, *16*, 309–319.
99. Bloznelis, S.M. Degree and clustering coefficient in sparse random intersection graphs. *Ann. Appl. Probab.* **2013**, *23*, 1254–1289.
100. Krishnan, B.; Ganesh, A.; Manjunath, D. On connectivity thresholds in superposition of random key graphs on random geometric graphs. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Istanbul, Turkey, 7–12 July 2013; pp. 2389–2393.
101. Krzywdziński, V.; Rybarczyk, K. Geometric graphs with randomly deleted edges—Connectivity and routing protocols. *Math. Found. Comput. Sci.* **2011**, *69*, 544–555.