A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security

Aditya Sundararajan

Aniket Chavan

Danish Saleem

Arif I. Sarwat

A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security

Aditya Sundararajan [1], Aniket Chavan [2], Danish Saleem [3] and Arif I. Sarwat [1,*]

[1] Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA; asund005@fiu.edu

[2] Electrical Engineering Department, Southern Methodist University, Dallas, TX 75275-0340, USA; achavan@smu.edu

[3] Energy, Security & Resiliency Center, Energy Systems Integration Facility, National Renewable Energy Laboratory, Golden, CO 80401, USA; Danish.Saleem@nrel.gov

* Correspondence: asarwat@fiu.edu; Tel.: +1-305-348-4941

Abstract: The increasing proliferation of distributed energy resources (DERs) on the smart grid has made distributed solar and wind two key contributors to the expanding attack surface of the network; however, there is a lack of proper understanding and enforcement of DER communications security requirements. With vendors employing proprietary methods to mitigate hosts of attacks, the literature currently lacks a clear organization of the protocol-level vulnerabilities, attacks, and solutions mapped to each layer of the logical model such as the OSI stack. To bridge this gap and pave the way for future research by the authors in determining key DER security requirements, this paper conducts a comprehensive review of the key vulnerabilities, attacks, and potential solutions for solar and wind DERs at the protocol level. In doing so, this paper serves as a starting point for utilities, vendors, aggregators, and other industry stakeholders to develop a clear understanding of the DER security challenges and solutions, which are key precursors to comprehending security requirements.

Keywords: DER; photovoltaic; wind turbine; communications; protocols; SCADA; standards; enforcement; challenges; solutions; security requirements

1. Introduction

The integration of distributed energy resources (DERs) such as wind and solar into the smart grid at the distribution level has been accelerating. These devices are equipped with sensing and actuating devices such as smart inverters, controllers, on-site Supervisory Control and Data Acquisition (SCADA), phasor measurement units (PMUs) and advanced metering infrastructure (AMI) smart meters. The multitude of these devices exploit different communications protocols and media to transmit information to utility command and control centers (CCCs) and receive control signals. With this growing ubiquity in sensing, communicating and acting, the corresponding vulnerabilities that can be potentially exploited also has been hiking [1–4]. Standards recommended by organizations such as the International Electrotechnical Commission (IEC) and the National Institute of Standards & Technology (NIST) have attempted to derive requirements and solutions to ensure strong and secure communications between grid-edge devices such as DERs and CCC applications such as the enterprise information system (EIS) or the integrated distribution management system [5–8]. However, in the United States, the recommendations of these standards have not been properly enforced by DER stakeholders, creating gaps resulting from customization that could be exploited by attackers.

Recent cyberattacks on the smart grid—including campaign efforts against Ukraine in 2015, 2016, and 2018 and the Dragonfly efforts against the western electric grid—suggest that security by obscurity is no longer a valid concept in securing digital assets [9–12]. Despite the sensitivity of communications infrastructure, the incorporation of stringent security controls and preventive measures that can withstand cyberattacks is subpar. Although the literature on power system aspects of DERs is exhaustive, the same cannot be said for that in the area of cybersecurity. In the future scenarios involving the use of DERs such as electric vehicles in grid-to-vehicle, vehicle-to-grid, and vehicle-to-vehicle modes of operation, and leveraging ancillary functions from DERs such as photovoltaic (PV) and energy storage in the form of dynamic grid support, primary frequency control, fault-ride through, intermittency response, and inertial response, raise concerns in the aspect of security at the customer level of the grid. Authors in [13,14] developed detailed models for vehicle-to-grid electric vehicles and utility-scale PV units, both equipped with fast-responding hybrid energy storage system, to support different ancillary services mentioned earlier. Considering their economical and performance viability, security paradigms—both centralized as well as distributed—must be explored. The use of edge and fog computing-driven security techniques would be better suited for such emerging scenarios [15]. Given a lack of clear organization of security requirements for DERs in such existing and emerging scenarios, the vendors employ different levels of security using proprietary methods, thus contributing to interoperability and standardization issues. Moreover, utilities currently have little to no operational visibility on remote DERs and, to compensate for it, rely on third-party vendors for monitoring, analytics and visualization, all of which in-turn depend on communication channels equipped with little or no encryption and other security precautions. Through multiple interviews with major utilities and DER vendors, different limitations of the current approach to DER security were discovered, presented here:

1. Most DERs communicate using Modbus or DNP3. Specifically, DERs such as smart inverters use Modbus, which is highly insecure since it employs no encryption. Communications from substation to the control center is typically on DNP3 which also has severe security deficiencies;

2. Vendors have access to utility OT networks for software/firmware updates, error reporting, performance monitoring, etc. This is highly insecure because a vendor (or an impostor) could successfully access other critical devices on the same network;

3. Manufacturers typically install Raspberry Pi-powered protection modules, and configure them to the Dynamic Host Configuration Protocol (DHCP) mode using which they communicate with the utility network;

4. Utilities also do not include cybersecurity requirements in their procurement language for DER equipment purchases because they assume the products come with adequate security mechanisms;

5. There is no mechanism today where patches or firmware get downloaded to an isolated system outside the OT network of concern, get inspected for data integrity and vulnerabilities, and only then be uploaded to the devices which need patching in the OT network;

6. Considering the minimal DER penetration into distribution networks currently, security is not given much importance, but with the increasing rate of integration of DERs, security at the device and protocol levels would be of utmost significance;

7. Regulatory guidelines such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) have defined cybersecurity requirements but only for the transmission grid systems. Moreover, co-operatives pay greatest attention just to NERC CIP, but in this new scenario, they must explore their security requirements beyond what is specified in the guidelines.

This paper has the following key contributions: (a) considering the above key shortcomings in the existing literature, it attempts to bridge the gap through its exhaustive survey with a special focus on DER protocol-level vulnerabilities, attacks, and solutions; (b) it provides a roadmap to ensure effective

security of DERs through the recommendation that compliance documentation should take the most basic and stringent security controls into account. Such documentation can accompany specifications mentioned in the IEC, Institute of Electrical and Electronics Engineers (IEEE), NIST, NERC, and other organizations developing standards to secure DER data and communications infrastructure; (c) it is one of the first few works to create a holistic conceptual distribution smart grid communications model that includes all the key devices from the grid edge to the command and control. This conceptual model also maps the protocols based on the Transmission Control Protocol/Internet Protocol (TCP/IP) stack to the Open Systems Interconnect (OSI) basic reference model that is more widely understood. In doing so, it serves as a single point of reference for researchers and industry members in the related areas; (d) contributes significantly to the gap in literature by providing a comprehensive documentation to the industry which compiles all the vulnerabilities of DERs—both PV and wind turbines—at the protocol level; and (e) it determines the gaps in achieving DER communications security requirements and introduces a layered defense model capable of addressing the gaps thus identified.

This paper is the first of two-part research effort summarized by the flowchart in Figure 1. This effort considers only two types of DER systems: PV and wind turbines. Further, their security requirements are considered from the purview of the distribution domain per the NIST smart grid architecture. The effort is conducted as a sequence of steps: (a) components of both DERs work over the TCP/IP stack; however, different devices use different protocols at each layer. The first step is to gather all these protocols at each layer; (b) because the OSI basic reference model is more widely understood, a mapping between the protocols identified in step (a) to the OSI layers is conducted for a more thorough review; (c) irrespective of the DER type, the vulnerabilities, attacks that exploit those vulnerabilities, and the solutions currently in the literature to mitigate such attacks are all common because they all depend on the protocols used. Hence, they are collectively reviewed; (d) following a review of vulnerabilities and attacks across all layers, the results are synthesized to derive the different PV and wind DER security requirements that the mitigation solutions must meet. It is also analyzed whether the existing solutions meet all of these requirements; (e) once the gaps between the capabilities of the existing solutions and the requirements are identified, a layered defense model is introduced to discuss how it can address the identified gaps; and, (f) finally, a validation process is designed through test cases to apply the proposed layered defense model to fulfill the unmet security requirements. Discussions about how the validated model can be used to ensure vendor DER compliance to the key security requirements are also included.

This paper considers only steps (a) through (c) for the first four layers of the OSI basic reference model: Physical, Data Link, Network, and Transport. The other layers, including the subsequent synthesis, are reserved for future work following the completion of this work (further described in Section 5).

The rest of the paper is organized as follows. Section 2 describes the communications infrastructure used by distributed PV and wind to communicate with the utility and the protocol-mapping between the TCP/IP and OSI models. Section 3 summarizes the key vulnerabilities of DER communications at the protocol level, which is studied using the OSI layers 1–4 as the reference. Section 4 highlights the potential cyber-attacks that can result from a successful exploitation of the vulnerabilities, and surveys the key solutions that exist in the literature to mitigate such attacks. Section 5 documents the second part of the research effort in greater detail. Finally, the paper's concluding remarks are documented in Section 6.
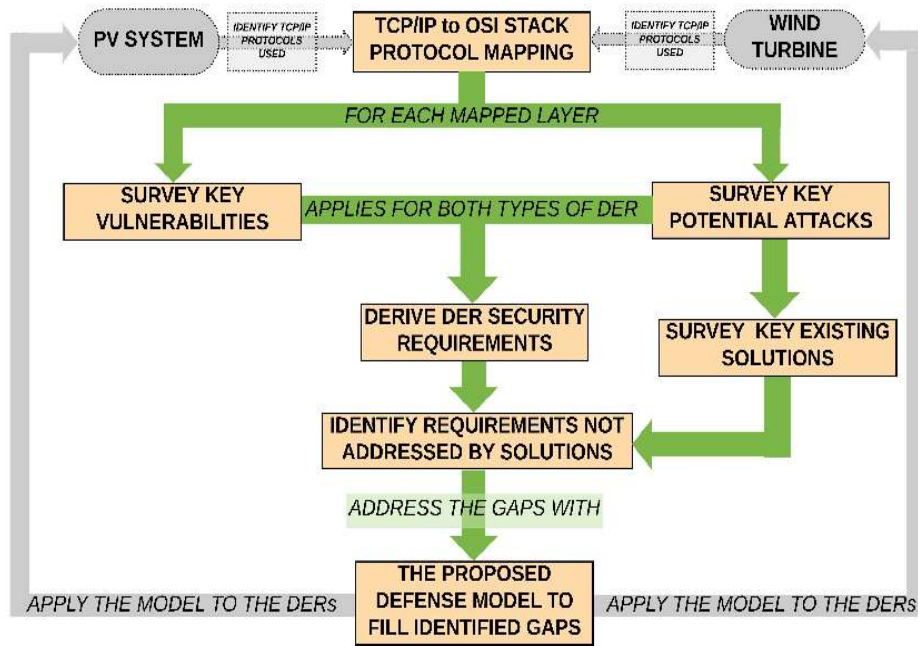
Figure 1. Flowchart showing the sequence of flow for the research effort.

2. DER Communications Architecture

This section examines the communications infrastructure used by PV and wind DERs to interact with utility CCCs. Key vulnerabilities in the communications are also defined and summarized.

Most smart grid devices communicate using application-layer protocols that work on a TCP/IP stack, which is a practical implementation of the theoretical, more well-known OSI Basic Reference Model. Hence, to understand how these protocols operate, a mapping between the TCP/IP stack and the OSI model must be understood. This mapping is shown in Figure 2. The TCP/IP stack, also called the Internet Protocol Suite or the U.S. Department of Defense model, has four layers of abstraction, and the OSI model has seven [16].
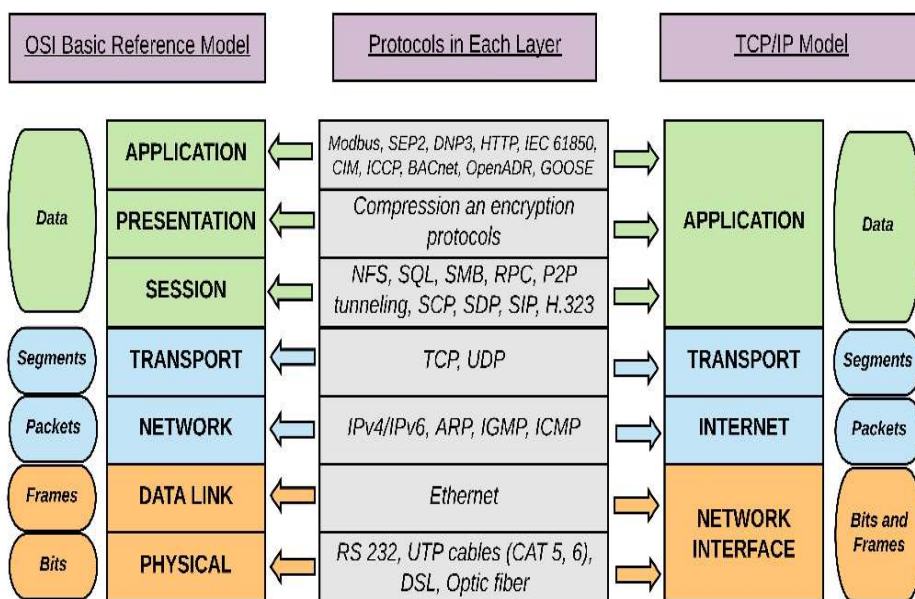

Figure 2. The logical mapping between OSI basic reference model and the TCP/IP stack.

2.1. Protocol Mapping

Although the OSI model is considered a reference model for network interconnection, the TCP/IP stack is considered, for all practical purposes, more effective in abstracting the communications. Developed primarily for connecting devices over the Internet, the TCP/IP stack facilitates point-to-point communications and prescribes how data must be framed, packeted, segmented, encoded/decoded, transmitted/received, and, finally, used for higher level user applications; however, the OSI model is more rigid in its definition of layers and does not pertain to the Internet networks.

Figure 2 that the Network Interface layer of the TCP/IP stack corresponds to the Physical and Data Link layers of the OSI model, the Internet layer serves a function similar to the OSI's Network layer, followed by the Transport layer, which is attributed commonly in both. Although the OSI model distinguishes the Sesssion, Presentation, and Application layers for establishing connections, sustaining context, and interfacing with the applications, the TCP/IP stack encapsulates these services into a single layer called the Application. Both the OSI model as well as the TCP/IP stack have been studied under the purview of security [17–22]. Tested security models such as defense-in-depth have been studied in the context of the TCP/IP stack [23]. It explored the use of physical security and Media Access Control (MAC) filtering for the Network Interface layer; the use of firewalls, access control lists (ACLs), and virtual private networks (VPNs) at the Internet layer, followed by Secure Socket Layer (SSL) or Transport Layer Security (TLS) at the Transport layer; and, finally, proxy- and host-based-firewalls and antimalware tools at the Application layer. However, this level of security is insufficient to counter sophisticated attacks such as those which targeting human users or those comparable to the advanced persistent threats (APTs). Recently, a security framework for the TCP/IP stack was proposed [24]. The work explored the use of 512-bit SF block ciphers and enhancing the Internet Control Message Protocol (ICMP) by leveraging the unused portion in the authentication field of the ICMP packet.

The OSI model's Physical layer encompasses the security of network devices from physical attacks, including from fire, water, tampering, cuts, and signal disruptions caused by interference. Role-based access control and data backups are some ways to ensure security at this layer. The Data Link layer is vulnerable to spanning tree attacks, MAC flooding and Address Resolution Protocol (ARP) poisoning. The Network and Transport layers include technologies such as IDS/IPS, firewalls, routers, and switches that encounter attacks such as denial of service (DoS), and unauthorized access, which can be protected against through ACLs and network address translation. Unauthorized data and account access are primary forms of threats confronting the Session and Presentation layers that can be countered using encryption and authentication. Application layer attacks include but are not limited to backdoor and malware exploits, social engineering, and malicious code injection. These attacks can be curbed to an extent through defense-in-depth strategies but more effectively by augmenting the model with strategies such as minimizing backdoors, regular version upgrades, awareness, and training [25–36].
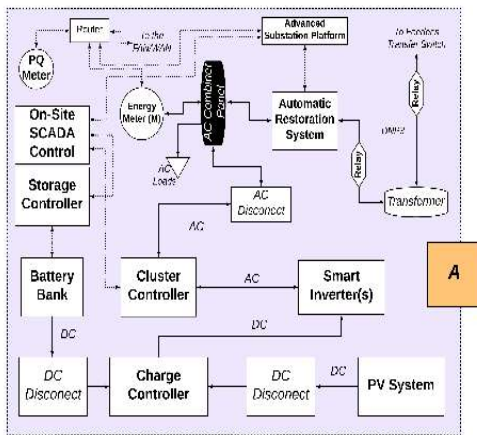
2.2. Architecture

Distributed PV can interact with the utility in different ways, as shown in Figure 3. The architecture is vertical, with grid-edge devices at the bottom and the CCC applications at the top. Distributed PV devices include smart inverters (which might be central plant inverters, string inverters, or micro-inverters), production meters that log the energy delivered by the system versus the energy drawn from the grid at the point of interconnection (POI) or point of common coupling, plant-level controllers that communicate directly with the SCADA, micro-PMUs or frequency disturbance recorders and weather stations (integrated with sensors) installed on-site. At the feeder level, multiple intelligent electronic devices (IEDs) such as reclosers, voltage regulators, capacitor banks, load tap changers, and switches monitor the feeder for changes in voltage and frequency. The AMI smart meters at the loads connected to the DERs and the DER's own production meter are part of a wider neighborhood area network that is used to transfer packets to access points. The feeder IEDs, meter access points and DER plant controllers all send data of different resolutions at different
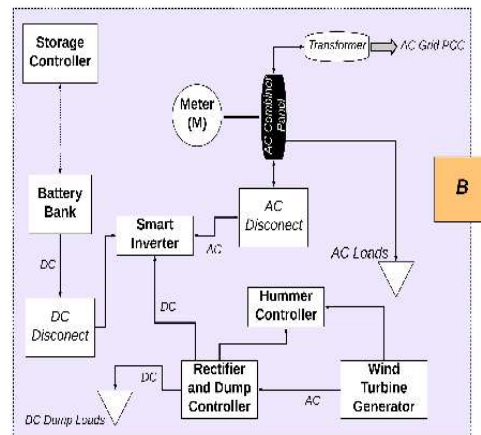
frequencies to the process bus, meter data concentrators, and facility DER management system (FDERMS), respectively, at the distribution substation.
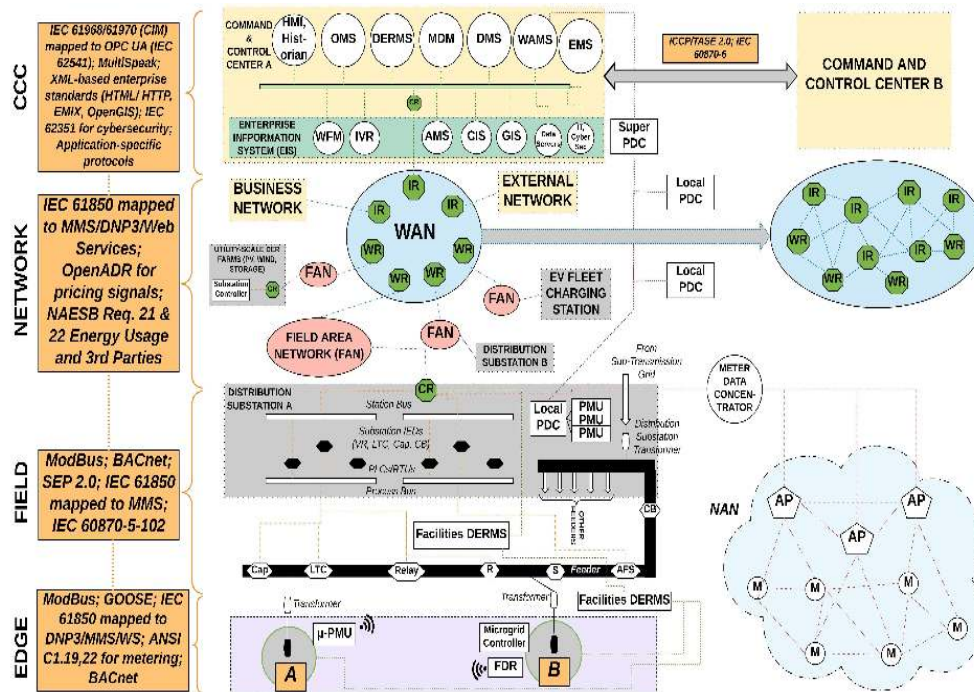
(**a**)

(**b**)　　　　　　　　　　　　　　　　　　　　　　　　(**c**)

Figure 3. (**a**) The high-level conceptual architecture of distributed PV and Wind DERs communicating with a CCC, along with the different communications protocols mapped to each layer; (**b**) a detailed schematic of distributed PV (A); and (**c**) A detailed schematic of a distributed wind turbine (B). Dotted lines represent communications flows, and solid lines or larger arrows denote power flows.

A cluster router at the substation bus aggregates the data and forwards it to the field area network (FAN), which bridges the gap between core IP devices and the field devices. Because of their large geographic coverage, FANs are deployed using wireless technologies such as cellular, both narrowband and broadband point-to-multipoint, and broadband wireless mesh networks [37]. FANs must ensure reliability, fault tolerance, and scalability, and, can be either dedicated to a single distribution substation, as shown in Figure 3, or expand across the utility territory. Additionally, FANs comprise FAN routers that can be deployed at the substation or on the field, and they use

protocols such as WiMAX, 900 MHz RF Mesh, 2G and 3G wireless, and WiFi [38–42]. Such routers enable grid operators to implement network security and also run SCADA protocol translation applications directly. Depending on the scale of the utility territory, wide area network (WAN) might be deployed, comprising gateway WAN routers at the edges and a mesh of internal routers within. Eventually, WAN routers at the utility's end exist; one for the business network, one for the external network, and one for the operational network [43–45]. EIS applications such as workforce and asset management, geographic information system (GIS) and customer information system, and enterprise cybersecurity technologies supplement the core enterprise applications of distribution management system (DMS), DERMS, energy management system, meter data management, outage management system, and the SCADA components such as the Historian and human machine interface (HMI), all of which interact over the enterprise bus [46–48].

Shown to the left are the different communications protocols identified for use by various devices at the Edge, Field, Network, and CCC, briefly elaborated in the following subsections.

2.2.1. Edge and Field

This encompasses the communications employed by the DER devices with those above them in the hierarchy. Typical protocols involved are Modbus, Building Automation and Control network (BACnet) at the edge, and the Advancing Open Standards for Information Security's (OASIS) Energy Market Information Exchange (eMIX) at the field [49–51]. Others include Smart Energy Profile (SEP) 1.x; object models from IEC 61850-7-420 and IEC 61850-90-7 mapped to Manufacturing Messaging Specification (MMS), Distribution Network Protcool (DNP) Version 3; SEP 2.0; or Web services through the Devices Profile for Web Services, Representational State Transfer, or web sockets [52–54]. The Modbus protocol has different subtypes: Modbus Remote Terminal Unit (RTU), TCP, or American Standard Code for Information Interchange (ASCII). Although Modbus RTU and ASCII work on serial, non-routable networks with a broadcasting mechanism, Modbus TCP works on the Application layer of the OSI basic reference model over a routable network, typically using Ethernet cables in unicast mode. Cybersecurity requirements for these protocols are as follows: none for Modbus, left to implementers for BACnet, inadequate for SEP 1.x and eMIX, IEC 62351 for IEC 61850 mapping to MMS, IEEE 1815 for IEC 61850 mapping to DNP3, WS-security and HTTPS for IEC 61850 mapping to Web services, and SEP 2.0 for IEC 61850 mapping to SEP 2.0. For the metering protocols of ANSI C12.19 and 22, the C12 security requirements apply [55].

SEP 2.0 is an international open standard that manages the energy of devices at homes and businesses. From minimizing peak, balancing the load and generation, to managing the operation of net zero buildings and microgrids, the protocol is used by utilities, aggregators, and consumers to securely install and maintain end devices with no additional configuration requirements [54]. It can be operated over any physical layer that supports IP-based protocols such as WiFi, ZigBee IP, Thread, Bluetooth, HomePlug, PLC, and Ethernet.

2.2.2. Network

F-DERMS at the substation level interacts with the DER SCADA at the distribution control center and DER aggregators over WAN-based information and communication technology (ICT) systems. F-DERMS in certain cases can also be replaced by microgrid energy management systems or microgrid control systems (MCSs) that support islanding features and on-demand dispatchability. Open Automated Demand Response (OpenADR) protocols find use here for demand response functionalities, and eMIX serves as a financial layer on top of the OpenADR for interaction with the energy market. OpenADR 2.0 facilitates information exchange between the utility and the customer and offers continuous dynamic pricing signals and automated demand response actions such as load shedding, direct load control, peak load shaving and shifting at customer levels. It uses standard-based IP transport mechanisms such as HTTP and XML Messaging and Presence Protocol (XMPP). Security has been integrated into OpenADR 2.0 across two levels: Standard, which uses TLS

to establish secure channels between a virtual top node and a virtual end node for communications, and High, which uses XML signatures for non-repudiation and documentation. IEC 61850 mapped to web services, DNP3, and MMS apply here as well.

Wireless protocols, part of the IEEE standards 802.11x—WiFi (IEEE 802.11), ZigBee (IEEE 802.15.4), and Bluetooth (IEEE 802.15.1)—are widely used by the Internet of things or industrial Internet of things sensors deployed at the Edge, Field, and Network layers of the grid. A prominent example of the use of ZigBee is by the AMI smart meters at the Edge to forward packets over their mesh network in the frequency of 868/915 MHz or 2.4 GHz.

2.2.3. CCC

At this level, the applications at the enterprise use the Common Information Model for interactions. IEC 61968 is used for the interactions among GIS, DMS, utility DERMS, OMS, and demand response, and IEC 61970 is used to exchange distribution power flow models. Inter-application messaging uses MultiSpeak, with its cybersecurity the responsibility of MultiSpeak Version 4. IEC 61968, IEC 61970, and enterprise standards such as HTTP, eMIX, and OpenGIS have no explicit cybersecurity specifications; however, Web services security and IEC 62541 can be used instead.

3. DER Communication Vulnerabilities

Considering different protocols are applied at different levels of the grid, with each layer covering multiple protocols, this section surveys the vulnerabilities with the OSI and GridWise Architecture Council (GWAC) layers at the focus. The OSI model's seven layers are augmented with the semantics and business context layers of the GWAC interoperability stack. This section discusses the key vulnerabilities of each layer that are summarized in Table 1, and the next section explores the attacks that exploit these vulnerabilities and the existing solutions [56,57].

Table 1. A Summary of DER Communication-Level Vulnerabilities Layers 1–4.

Layer	Layer Number	Protocols/ Connections	Smart Grid Layer(s)	Standard/ Body	Vulnerabilities
Physical [58–65]	Layer 1	RS 232, UTP cables (CAT 5, 6), DSL, optic fiber	Edge, Field, Network	IEEE 802.3	Data/hardware thefts, unauthorized changes to functional environment, undetectable data interception, wiretaps, and reconnaissance, open authentication, rogue employees and access points
Data Link [66–72]	Layer 2	Ethernet	Edge, Field	IEEE 802.1, IEEE 802.3	Unauthorized joins and expansion of the network, VLAN join, tagging and hopping, remote access of LAN, topology and vulnerability discovery, break-ins, switch control
Network [73–82]	Layer 3	IPv4/IPv6	Edge, Field	IETF	Guessing TCP sequence numbers, stealing existing session, no cryptography
		ARP			No authentication, works in broadcast
		IGMP, ICMP			Unauthorized access
Transport [83–92]	Layer 4	TCP, UDP	All	IETF, DARPA	Three-way handshake flaws, TCP sequence number prediction, port scan

3.1. Physical (Layer 1)

As briefly described in Section 2.1, the Physical layer includes the devices and the channels used for communications among devices. Such channels include connectors and cables such as RS-232,

CAT 5/6, Digital Subscriber Link (DSL), or optic fibers. This layer is vulnerable to thefts where sensitive data could be stolen by the attacker through efforts such as changing the configuration settings, altering the calibration, or simply damaging the equipment [58–60]. The connections between two devices might also be subjected to physical attacks that range from unplugging cords or cables to unauthenticated or unauthorized devices, damaging or severing the channels physically, or simply removing connections to the legitimate devices. Wiretapping and open authentication mechanisms are vulnerabilities that allow the attacker to gain access to the network directly [61,62]. The access points could deliberately be turned rogue by an attacker to potentially exploit for man-in-the-middle (MITM) attacks. With humans being the weakest link in a cybersecurity kill chain, insider threats could manifest as rogue or disgruntled employees connecting to the remote DER devices through legitimate Bluetooth or speedwire connections and engaging in thefts, manipulation, or damage of the data or device. In addition to man-made causes, the same vulnerabilities could be exploited by natural means triggered by exposure of the DER devices to inclement weather, including extremities such as storms and lightning strikes [63–65].

3.2. Data Link (Layer 2)

Some protocols on this layer are Ethernet, Frame relay, and Asynchronous Transfer Mode. Among them, Ethernet is found to be used predominantly by all DER communications at this layer [66–68]. Hence, the other protocols on this layer will be considered beyond the scope of this paper. Using an unconnected port on a switch, any device can join the network's Ethernet segment. It might also exploit the fact that upon disconnection of the host from a network, the connection between the socket and switch is not lost, thereby leaving wall sockets connected to switches. The network can be expanded without authorization by installing one's own wireless access points and switches and adding other users to them [69–72].

3.3. Network (Layer 3)

This layer defines the path for a packet that might pass through different intermediary devices in the communications infrastructure. The primary protocols at this layer include IPv4/IPv6, ICMP, ARP, and the Internet Group Management Protocol (IGMP) [73–77]. The IP packets are found to transmit data in a plaintext format, and the ARP packets are susceptible to be exploited by the attacker because of the lack of authentication. This lack of authentication can enable rogue device connections such as compromised computers, access points, switches, or routers. The lack of encryption and authentication makes protocols on this layer vulnerable to flooding, poisoning, and spoofing attacks. The mitigation strategy currently employed by IPv4 against ICMP flooding is to drop all incoming ICMP packets because they do not affect the network functionality. However, this strategy cannot be applied to IPv6 because it uses ICMP for neighbor discovery and path maximum transmission unit [78–82].

3.4. Transport (Layer 4)

At this layer, two types of connections can be made: TCP or User Datagram Protocol (UDP). TCP requires acknowledgment for establishing connection but UDP does not. While the IP establishes the connection across the network, the port defines the type of connection and the protocol used by that connection. The first (FIR) and end (FIN) control flags of the segment can be exploited. The FIR and FIN flags indicate the first and final frames of the segment, respectively. When a message with the FIR flag arrives, all previously received incomplete segments are discarded. Inserting a message with the FIR flag set after the beginning of a transmission of a segmented message causes the reassembly of a valid message to be disrupted. Inserting a message with the FIN flag set terminates the message reassembly early, resulting in an error during the processing of the partially completed message [83–87]. The Sequence field used to ensure in-order delivery of the segmented messages is also vulnerable to attacks. The sequence number increments with each segment sent, so predicting the next value is trivial. An attacker who inserts fabricated messages into a sequence of segments can

inject any data and/or cause processing errors. The ports are vulnerable to either banning or scanning. Port banning occurs when the accessed port provides information on the protocol running on the port, the device's operating system and application, etc. Port scanning helps the attacker in obtaining valuable information of the network, including IP address, list of open ports and the applications running on those ports [88–92].

4. Potential Cyberattacks and Corresponding Solutions to Secure DER Communications

Following the survey of the vulnerabilities, different attacks that could potentially exploit these vulnerabilities are discussed in this section, followed by a brief summary of existing solutions to mitigate them. The information is summarized in Table 2.

Table 2. A Summary of DER Communication-Level Attacks and Existing Solutions Layers 1–4.

Layer	Layer Number	Protocols/ Connections	Potential Attacks	Existing Solutions
Physical [57,62,93–96]	Layer 1	RS 232, UTP cables (CAT5/6), DSL, optic fiber cables	Stealing data, data slurping, wiretapping, Bluejacking and Bluesnarfing, physical destruction, obstruction, manipulation of physical assets	Block the USB port, data storage cryptography, accountability and auditing to track and control physical assets [57,62,96]
Data Link [71,97–106]	Layer 2	Ethernet	ARP poisoning, MAC flooding and spoofing, spanning-tree, multicast brute force, identity theft, attacks on VLAN trunking protocol and VLAN hopping, double-encapsulated 802.1Q/nested VLAN attacks	Physical protection, network segmentation, role-based access control, ACLs, control and management plane overload protection, centrally managed LAN security, encryption and integrity verification, Ethernet firewall and deep packet inspection, IDPS, port security, packet storm protection [103–106]
Network [107–115]	Layer 3	IPV4/IPv6	Spoofing, teardrop, replay, wormhole, routing, network manipulation and consumption, MITM, DoS	Use: firewalls, packet filters, application/circuit-level gateways, proxy servers, net/IPFilters, two-way authentication, network/protocol/ host-IDS [111–113,116]
		ARP	Spoofing, also known as cache poisoning	Authenticated IP addresses, modifying ARP using cryptographic techniques, manual configuration of static ARP entries [115]
		IGMP, ICMP	ICMP flooding, Smurf attack	Rate-limit traffic, turnoff ping [114]
Transport [117–125]	Layer 4	TCP, UDP	TCP hijacking, TCP SYN flooding, UDP flooding	Use: SSL/TLS, secure cookie flags, HTTP strict transport security, public key pinning, strong keys, efficient key management, certificates with required domain names and fully qualified names; do not use: sensitive data in URLs or caches, wildcard certificates [122–125]

4.1. Physical (Layer 1)

Data or device thefts, data slurping, and wiretapping are commonly observed attacks at this layer. The Bluetooth Physical layer can be compromised through Bluejacking and Bluesnarfing attacks [93]. Physical destruction, obstruction, or manipulation could result in malfunctioning of the physical assets in the DER environment, primarily because of their exposed installations at remote locations where operational visibility might be poor or none [94]. This increases the cost to repair or reinstall and the cost for crew dispatch, both at the expense of increased service downtime [95].

These attacks could be mitigated in different ways: (1) blocking or hardening the unused Universal Serial Bus (USB) ports; (2) using data storage cryptography to protect sensitive data to at least prevent the loss of data confidentiality or integrity if the theft is successful; and (3) employing additional security methods such as ACLs to ensure accountability, and auditing to track and control the DER

devices. Additionally, to mitigate physical attacks, the devices could be installed in enclosures secured by locks and keys, or could be physically isolated from other frequently used infrastructure in the area, guarded by fences or gates [57,62,96].

4.2. Data Link (Layer 2)

Ethernet, the key protocol used at this layer by DERs is susceptible to a wide array of attacks, such as MAC flooding, MAC spoofing, or virtual local area network (VLAN) hopping. The MAC address can be spoofed to make the switch send Ethernet frames to the attacker's machine [97–100]. Irrespective of the security measures deployed at higher layers, a successful MAC spoofing still compromises the target device. The MAC address table used by a switch to store the MAC addresses of different devices, each connected to a specific port of that switch, could be subjected to a flooding attack triggered by the attacker, which results in overuse of memory, potential bottlenecks in communications that in turn causes delays or a drop of legitimate MAC addresses from the table. Hence, MAC flooding can be viewed as a DoS attack at this layer [71,101,102].

Different solutions currently exist to counter attacks at this layer. Some include port security to configure switches and enable them to learn a limited number of MAC addresses; and deploying an Authentication, Authorization and Accounting server to mediate network connections and ensure that the MAC addresses are added to the table only after they have been authenticated, authorized, and accounted for. Role and authentication-based access controls are key strategies to prevent attacks of this nature. Segmentation of VLANs, link-layer encryption, and integrity validation techniques could also be of help [103–106].

4.3. Network (Layer 3)

False ARP requests could be sent by an attacker in the network, enabling them to link their MAC address with the IP address of a different authorized device or system. Such an attack is labeled ARP spoofing, possible because of the exploitation of the vulnerability of no authentication [107–110]. ICMP and ping flooding attacks overload the target IP addresses by a sudden influx of data packets. Ping requests or ICMP packets are transmitted over the network to check for connectivity, which could be exploited using tools such as hping and scapy. The data in plaintext could be used by an attacker to engage in different attacks ranging from sniffing or theft to more malicious ones such as MITM or packet replay.

The ping request and ICMP flooding can be mitigated by turning pings off from external networks and rate-limiting the ICMP traffic, respectively, to prevent the bandwidth and firewall performance from being impacted [111–114]. Attacks exploiting plain-text data can be avoided by using security architecture such as IP-Sec or transport access control [115]. The authors in [116] propose a fuzzy logic based model to mitigate DoS-style attacks against vehicular Ad hoc networks. This model extends the analysis of greedy routing for packet forwarding and is capable of selecting the best next-hop node in multi-hop vehicular Ad hoc networks. Two routing metrics are given as inputs to the fuzzy decision-making model for each of the neighbor nodes to select the best next-hop neighbor node based on the output of the fuzzy model.

4.4. Transport (Layer 4)

This layer is greatly susceptible to attacks that target the TCP or UDP, such as SYN flooding or UDP flooding. In SYN flooding, the attacker uses fake IP addresses to send continuous SYN requests to the target device on its different ports. Assuming all requests as genuine, the target system sends the acknowledgment (SYN_ACK) packets to each requesting fake IP. This creates a scenario where the port remains open until the connection times out, when another fabricated SYN request is received. This overwhelms the target system's resources and prevents legitimate users from establishing connections [117–121]. Although UDP does not need a handshake to establish a

connection, which in itself creates a vulnerability for attacks that overwhelm the connections with large volumes of bogus traffic.

SYN flooding is prevented using methods such as cryptographic hashing where the target device sends the SYN_ACK packet with a sequence code derived from the requesting client's IP address, port number, and a unique identification number. Stack tweaking can also be used, which reduces the connection request timeout period or resorts to random dropping of incomplete connections. UDP flooding is typically prevented by rate-limiting the UDP packets [122–125].

4.5. Key Observations

At each layer, a few attacks have been observed to show more prevalence in the literature. Some of the most prominent attacks include MAC flooding, which could target any device in the DER environment that has a valid MAC address and uses Ethernet in the Data Link layer. Such devices include but are not limited to inverters, control systems, smart meters, synchrophasors, network switches, routers, and other communications gateways. Port security in the form of hardening unused ports and predefining the number of MAC addresses on a particular switch port are the most effective solutions currently recommended by the industry to prevent attacks of such nature.

In devices that use IP addresses, spoofing is typically observed the most. Unauthorized access to the network can be gained by attackers by changing the source IP address in the IP packet header. The industry currently recommends the use of router-based IP filters to map the incoming traffic interface with designated interface of the source IP address present in the MAC address table. Many Intrusion Detection and Prevention Systems (ID/IPS) and inline blocking tools are also capable of detecting bad ARP messages and ensuring the stability and availability of the MAC address table.

MITM and packet replays are commonly observed attacks in DER devices where the set-point commands and other modification requests originating from the client applications using TCP or UDP could be intercepted and/or manipulated. These commands and requests have been observed to be in plaintext, thereby making these attacks prevalent. A particular use case of replay attack that retransmitted a legitimate plaintext set-point command after modifying it bypassed the DER client credentials and was successfully accepted by the device [126]. Different cryptographic techniques can prevent MITM and replay attacks considering the use of strong key distribution and exchange schemes [127]. It has also been shown through research that DER applications using TCP-based communications, by virtue of their three-way handshake and inclusion of the sequence number in their header, are less susceptible to replay than those using UDP.

DoS or distributed Dos (DDoS) attacks target DERs in three observed ways: volume, protocol, or application. The primary characteristic targeted is availability of services, which could be the availability of power or communications or data itself. Although volume-based DoS aim to overwhelm the device or communications channel by sending large volumes of requests or messages to reduce the availability of power or data, protocol-based attacks aim to cripple the underlying communications protocols by manipulating the payload or headers, thereby impacting the availability of the communication channel or medium. The application-layer-based DoS attacks target the client applications interacting with the DER devices, where the availability of data is compromised. The most widely employed methods to secure devices and networks against DoS/DDoS-style attacks include firewalls, ID/IPS, traceback and push-back services, and packet filters that limit the rate of traffic.

5. Future Work

This section first summarizes the second part of the research effort, which will be conducted by the authors moving forward. Then, the significant results derived from this survey are discussed.

5.1. Surveying Layers 5 through 7, GWAC Interoperability Stack

It has been identified in the literature that the OSI model's 7 conceptual layers are insufficient to prevent higher level attacks, which are perpetrated by intelligent attackers and exploit the

vulnerabilities of human users and employ persistent methods to stay latent in the domain. To this effect, the OSI model is augmented with the GWAC interoperability stack's top two layers of semantic and business for interoperability and policies and governance for organizational security; however, these additional layers bring their own security-related challenges, including those because of interoperability, an increased number of attack entry points, the likelihood of compromise of privacy and confidentiality, and more [128,129].

The second part of the research effort will explore the protocol-level vulnerabilities, potential attacks, and existing solutions at OSI layers 5 (Session), 6 (Presentation), and 7 (Application) as well as GWAC stack drivers of Semantics and Business. The basic and advanced security requirements will be revisited and refined based on the insights derived from this survey. The proposed layered defense model introduced in the following subsection will be elaborated, and its application in meeting these requirements will be discussed. The model has already been integrated into and validated over the Security & Resilience (S&R) networking testbed at the National Renewable Energy Laboratory (NREL) by the authors. As future work, the test cases designed to validate the basic and advanced controls to ensure DER security will be validated on the S&R testbed in the presence of the layered defense model, and the results will be documented.

5.2. Introducing the Significance of NREL's Layered Defense Model for DER Security

Following the review of protocol-level vulnerabilities of DERs, the potential attacks that can exploit those vulnerabilities, and the solutions existing to counter those attacks, a set of security requirements have been developed by the authors to ensure security of data and communications in the DER domain. These requirements are categorized into *basic* and *advanced* security controls as shown in Figure 4. Although basic controls are the best practices for DER networks that are not specific to the DER devices, the advanced controls are required to be adhered to by a given communications or interconnection standard. These controls are described briefly as follows:

The basic security controls include:

1. Strictly implementing role-based access controls on the DER devices and network components;
2. Employing sound network segmentation principles to create different VLANs for information technology, operational technology and business networks;
3. Conducting regular upgrades of patches to the application software or DER firmware and ensuring that an effective patch management process is in place;
4. Using strong passwords that are immune to dictionary attacks and password cracking, including modifying the default passwords that the DER devices are assigned at the time of manufacturing/installation;
5. Employing selective encryption to reduce the processing overhead incurred in the encryption and decryption steps, considering that the DER devices are located at remote fields and are resource-constrained;
6. Padding the DER devices with network front-ends such as inline blocking and protocol-level filtering tools that validate the integrity of incoming and outgoing messages before being passed onto the actual devices;
7. Practicing strong port-hardening techniques such as disabling unused ports and closely monitoring the active ports available for connection to different client application requests.

The advanced security controls include:

1. Employing TLS versions 1.2 or 1.3 and recommended cipher suites to comply with the NIST guidelines;
2. Supporting session resumption that uses a secret session key for scenarios where the session stays disconnected for a time less than the TLS session resumption time;
3. Supporting session renegotiation that uses a secret session key for scenarios where the session stays disconnected for a time more than the TLS session renegotiation time;

4. Supporting the use of message authentication codes and multiple certificate authorities when communicating across DER domains;
5. Maintaining an active certificate revocation list to bar connection requests coming from entities with expired or blacklisted certificates.
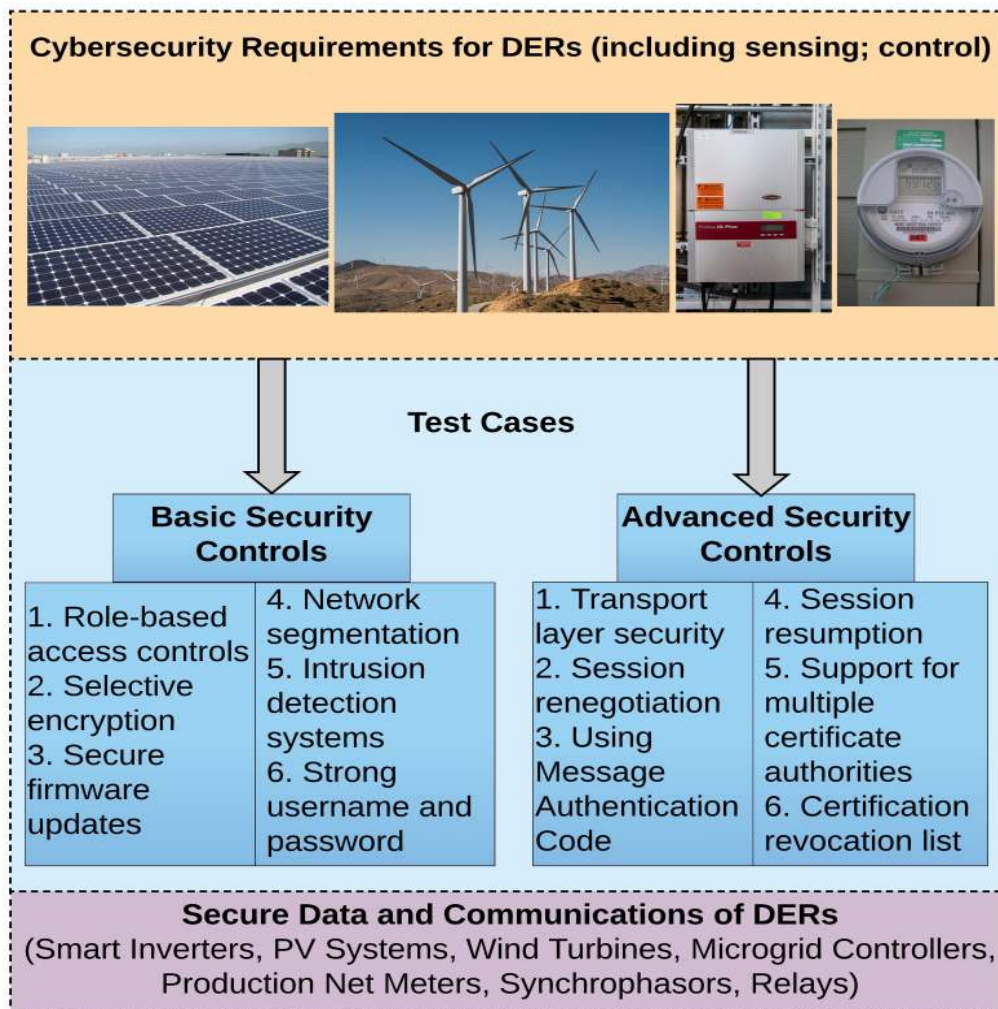

Figure 4. The DER security requirements derived from the survey in Sections 3 and 4. Figure numbers from left to right: NREL 19487 (PV system), NREL 50709 (wind farm), NREL 45576 (smart inverter), and NREL 21394 (smart meter).

Contrasting the existing solutions from Table 2 with these requirements above shows that there exists a gap in research. Although the solutions rely primarily on security technologies such as firewalls and ID/IPS, principles like strong passwords and access controls, and mechanisms for ensuring authentication and authorization, they are insufficient against sophisticated attacks such as APTs and social engineering. These traditional solution methods have a common goal of attack prevention but do not focus on event detection and incident response, which are crucial to countering future attacks.

Specifically, the existing solutions proposed by certain vendors cover basic requirements 1 and 7, and advanced requirement 4; however, these solutions must be augmented with advanced inline blocking, message filtering down to the hardware-level and anomaly-detection tools, using selective encryption and cipher suites, and enabling strong stakeholder engagement among different DER actors such as owners, aggregators, installers, and end-users. Additionally, at a central level,

intelligence-driven learning algorithms and data analytics can be used to detect and respond to potential threats to the DERs proactively. These suites of active methods have been accounted for by the layered defense model.

6. Conclusions

This paper dealt with the first of a two-part research effort to develop an organization of the existing literature in the domain of DER communications security at the distribution smart grid level. This paper focused on OSI layers 1 through 4, and the next paper will deal with OSI layers 5 through 7 and GWAC interoperability stack drivers 2 and 3, making for a comprehensive review of the protocol-level vulnerabilities of all eight layers, potential attacks that could exploit those vulnerabilities, and solutions proposed in the existing literature to mitigate such attacks. Given the application-level protocols used in the DER domain work on the TCP/IP stack, a mapping of protocols from the TCP/IP stack to the OSI model was made to gain a more conceptual understanding of the security challenges and solutions. Based on the survey, a high-level summary of the different basic and advanced security control requirements derived to ensure DER data and communications security were discussed. By contrasting the existing solutions for layers 1–4 against the requirements derived for the same, it was concluded that they are insufficient against APTs and social engineering attacks that exploit flaws in enforcement and human weaknesses to detect and respond to attacks.

References

1. INL. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*; Idaho National Laboratory (INL) Mission Support Center Analysis Report; Idaho National Laboratory: Idaho Falls, ID, USA, 2016.
2. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. *J. Electr. Syst. Inf. Technol.* **2018**. [CrossRef]
3. Ozgur, U.; Nair, H.T.; Sundararajan, A.; Akkaya, K.; Sarwat, A.I. An Efficient MQTT Framework for Control and Protection of Networked Cyber-Physical Systems. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017.
4. Eder-Neuhauser, P.; Zseby, T.; Fabini, J.; Vormayr, G. Cyber attack models for smart grid environments. *Sustain. Energy Grids Netw.* **2017**, *12*, 10–29. [CrossRef]
5. NIST. *NISTIR Guidelines for Smart Grid Cybersecurity Revision 1*; NIST: Gaithersburg, MD, USA, 2014.
6. D.O.E. *Cybersecurity Capability Maturity Model Version 1.1.*; U.S. DOE Technical Report; U.S. Department of Energy: Washington, DC, USA, 2014.
7. NERC. *Improving Human Performance: From Individual to Organization and Sustaining the Results*; North American Electric Reliability Corporation (NERC) Technical Presentation; NERC: Atlanta, GA, USA, 2012.
8. Benoit, J. *Making Sense Out of Smart Grid Cyber Security Standards*; White Paper by Cooper Power Systems; Eaton: Cleveland, OH, USA, 2013.
9. Lee, R.M.; Assante, M.J.; Conway, T. *CrashOverride: Analysis of the Threat to Electric Grid Operations*; Dragos Technical Report; Dragos Inc.: Hanover, MD, USA, 2016.

10. SANS. *The Impact of Dragonfly Malware on Industrial Control Systems*; SANS Institute InfoSec Reading Room Technical Report; SANS Institute: Singapore, 2016.

11. US-CERT. *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*; US Computer Emergency Readiness Team (CERT) Alert (TA18-074A); US-CERT: Washington, DC, USA, 2018.

12. Dragos. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; SANS Industrial Control Systems Electricity Information Sharing and Analysis Center Technical Report; Dragos Inc.: Hanover, MD, USA, 2017.

13. Hernandez, J.C.; Bueno, P.G.; Rus-Casas, C. Enhanced utility-scale photovoltaic units with frequency support functions and dynamic grid support for transmission systems. *IET Renew. Power Gener.* **2017**, *11*, 361–372. [CrossRef]

14. Hernandez, J.C.; Sanchez-Sutil, F.; Vidal, P.G.; Rus-Casas, C. Primary frequency control and dynamic grid support for vehicle-to-grid intransmission systems. *J. Electr. Power Energy Syst.* **2018**, *100*, 152–166. [CrossRef]

15. Anzalchi, A.; Sundararajan, A.; Wei, L.; Moghadasi, A.; Pour, M.M.; Sarwat, A.I. Future Directions to the Application of Distributed Fog Computing in Smart Grid Systems. *Smart Grid Anal. Sustain. Urban* **2018**. [CrossRef]

16. Zimmerman, H. OSI Reference Model-The IS0 Model of Architecture for Open Systems Interconnection. *IEEE Trans. Commun.* **1980**, *28*, 425–432. [CrossRef]

17. Surman, G. *Understanding Security Using the OSI Model*; SANS Institute InfoSec Reading Room Technical Report; SANS Institute: Singapore, 2002.

18. Buffenoir, T. A Layered Security Model: OSI and Information Security. *Comput. Stand. Interfaces* **1988**, 145–150. [CrossRef]

19. Holl, K. *OSI Defense in Depth to Increase Application Security*; SANS Security Essentials GSEC Practical Assignment Version 1.4b; SANS Institute: Singapore, 2003.

20. Pace, K. *A Layered Security Model: OSI and Information Security*; SANS Institute Global Information Assurance Certification Paper; SANS Institute: Singapore, 2004.

21. Bellovin, S. Security Problems in the TCP/IP Protocol Suite. *Comput. Commun. Rev.* **1989**, *19*, 32–48. [CrossRef]

22. Mateti, P. Security Issues in the TCP/IP Suite. In *Security in Distributed and Networking Systems*; World Scientific Review Volume: Singapore, 2006.

23. Dominguez, J. *An Overview of Defense in Depth at Each Layer of the TCP/IP Model*; SANS Institute Global Information Assurance Certification Paper; SANS Institute: Singapore, 2002.

24. Kumar, M.; Karthikeyan, S. An Enhanced Security for TCP/IP Protocol Suite. *Int. J. Comput. Sci. Mob. Comput.* **2013**, *2*, 331–338.

25. Idaho National Laboratory (INL). *Control Systems Cyber Security: Defense in Depth Strategies*; Idaho National Laboratory (INL) Control Systems Security Center Technical Report; Idaho National Laboratory: Idaho Falls, ID, USA, 2006.

26. Small, P. *Defense in Depth: An Impractical Strategy for Cyber World*; SANS Institute InfoSec Reading Room Report; SANS Institute: Singapore, 2011.

27. SANS Institute. *Defense in Depth*; SANS Institute InfoSec Reading Room Report; SANS Institute: Singapore, 2001.

28. Shamim, A.; Fayyaz, B.; Balakrishnan, V. Layered Defense in Depth Model for IT Organizations. In Proceedings of the 2nd International Conference on Innovations in Engineering and Technology, Bengaluru, India, 21–23 August 2014.

29. Sundararajan, A.; Khan, T.; Aburub, H.; Sarwat, A.I.; Rahman, S. A Tri-Modular Human-on-the-Loop Framework for Intelligent Smart Grid Cyber-Attack Visualization. In Proceedings of the IEEE Southeast Conference, St. Petersburg, FL, USA, 19–22 April 2018.

30. Intergraph. *Smart Grid Operations Command-and-Control Center: Bringing a Common Operating Picture to the Control Room*; Intergraph Technical Report: Solution Sheet; Intergraph: Madison, AL, USA, 2010.

31. Anzalchi, A.; Sarwat, A. A survey on security assessment of metering infrastructure in Smart Grid systems. In Proceedings of the SoutheastCon 2015, Ft. Lauderdale, FL, USA, 9–12 April 2015; pp. 1–4. [CrossRef]

32. Kott, A.; Wang, C.; Erbacher, R. *Advances in Information Security. Cyber Defense and Situation Awareness*; Springer: Berlin, Germany, 2014.

33. Wei, L.; Moghadasi, A.H.; Sundararajan, A.; Sarwat, A.I. Defending mechanisms for protecting power systems against intelligent attacks. In Proceedings of the 2015 10th System of Engineering Conference (SoSE 2015), San Antonio, TX, USA, 17–20 May 2015; pp. 12–17. [CrossRef]

34. Kott, A.; Lange, M.; Ludwig, J. Approaches to Modeling the Impact of Cyber Attacks on a Mission. *arXiv* **2017**, arxiv:1710.04148

35. Ibrahim, E. *A Layered Solution to Cybersecurity*; National Renewable Energy Laboratory (NREL) Technical Paper; National Renewable Energy Laboratory (NREL): Golden, CO, USA, 2017.

36. Ibrahim, E. Disruptive Ideas for Power Grid Security and Resilience with DER. In Proceedings of the National Renewable Energy Laboratory Annual Cybersecurity and Resilience Workshop, Golden, CO, USA, 9–10 October 2017.

37. Cisco. *Unified Field Area Network Architecture for Distribution Automation*; Cisco Technologies White Paper; Cisco: San Jose, CA, USA, 2014.

38. SEP. *Communication Network Challenges and Solutions in the Utility Industry*; Sierra Energy Group's Research & Analysis Division of Energy Central Technical White Paper Report; Sierra Energy: Davis, CA, USA, 2011.

39. Rodine, C. *The Field Area Network (FAN)*; Electric Power Research Institute (EPRI) Technical Presentation at Stanford University; Electric Power Research Institute (EPRI): Palo Alto, CA, USA, 2011.

40. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the 8th International Conference on Information Technology (ICIT), Bhubaneswar, India, 21–23 December 2017.

41. Elyengui, S.; Bouhouchi, R.; Ezzedine, T. The Enhancement of Communication Technologies and Networks for Smart Grid Applications. *Int. J. Emerg. Trends Technol. Comput. Sci.* **2013**, arXiv:1403.0530v1.

42. Mendes, T.D.P.; Godina, R.; Rodrigues, E.M.G.; Matias, J.C.O.; Catalão, J.P.S. Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources. *Energies* **2015**, *8*, 7279–7311. [CrossRef]

43. Sarwat, A.I.; Sundararajan, A.; Parvez, I. Trends and Future Directions of Research for Smart Grid IoT Sensor Networks. In *International Symposium on Sensor Networks, Systems and Security*; Springer: Cham, Germany, 2017; pp. 45–61.

44. SunilKumar, K.N.; Shivashankar. A review on security and privacy issues in wireless sensor networks. In Proceedings of the 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Piscataway, NJ, USA, 19–20 May 2017. [CrossRef]

45. Robertson, P.; Gordon, C.; Loo, S. Implementing Security for Critical Infrastructure Wide-Area Networks. In Proceedings of the Power and Energy Automation Conference, Spokane, WA, USA, 26–28 March 2013.

46. ESRI. *Enterprise GIS and the Smart Electric Grid*; ESRI Technical White Paper; ESRI: Redlands, CA, USA, 2009.

47. Parra, I.; Rodriguez, A.; Arroyo-Figueroa, G. Electric utility enterprise architecture to support the Smart Grid-Enterprise architecture for the Smart Grid. In Proceedings of the 11th International Conference on Informatics in Control, Automation and Robotics (ICINCO), Vienna, Austria, 2–4 September 2014.

48. Parekh, K.; Zhou, J.; McNair, K.; Robinson, G. Utility Enterprise Information Management Strategies. In Proceedings of the Grid-Interop Forum, Albuquerque, NM, USA, 7–9 November 2007.

49. Modbus Application Protocol Specification V 1.1b3. Avaiable online: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf (accessed on 2 September 2018).

50. ASHRAE. *BACnet—A Data Communication Protocol for Building Automation and Control Networks*; ANSI ASHRAE Standard Specification; ASHRAE: New York, NY, USA, 2008.

51. OASIS. *Energy Market Information Exchange (EMIX) Version 1.0.*; OASIS Committee Specification 02; OASIS: Burlington, MA, USA, 2012.

52. ABB. *DNP3 Communication Protocol Manual*; ABB Technical Report Version 1.1.; ABB: Zurich, Switzerland, 2011.

53. IEEE. *1815.1-2015—IEEE Standard for Exchanging Information between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]*; IEEE Standards Document; IEEE Power & Energy Society: Piscataway, NJ, USA, 2016.

54. IEEE. *P2030.5—IEEE Approved Draft Standard for Smart Energy Profile Application Protocol*; Revision of IEEE Standard 2030.5-2013; IEEE: Piscataway, NJ, USA, 2018.

55. East, S.; Butts, J.; Papa, M.; Shenoi, S. A Taxonomy of Attacks on the DNP3 Protocol. In Proceedings of the International Conference on Critical Infrastructure Protection, Hanover, NH, USA, 23–25 March 2009. [CrossRef]

56. Ramaswamy, R. Traffic flow confidentiality security service in OSI computer network architecture. In Proceedings of the IEEE TENCON'90: 1990 IEEE Region 10 Conference on Computer and Communication Systems, Hong Kong, China, 24–27 September 1990. [CrossRef]

57. Childers, M.; Borrielli, M. IEC61850 substation experiences DPSP 2012. In Proceedings of the 11th IET International Conference on Developments in Power Systems Protection (DPSP), Birmingham, UK, 23–26 April 2012. [CrossRef]

58. Alzari, A.S. Telecommunication traffic through submarine cables: Security and vulnerabilities. In Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016. [CrossRef]

59. Luo, G. Wireless transmission of RS232 interface signal based on ZigBee. In Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, Chengdu, China, 18–20 July 2010. [CrossRef]

60. Hu, S.; Sun, J. Research on the network security based on radiated virus. In Proceedings of the 2010 International Conference on Information, Networking and Automation (ICINA), Kunming, China, 18–19 October 2010. [CrossRef]

61. Oberle, A.; Larbig, P.; Kuntze, N.; Rudolph, C. Integrity based relationships and trustworthy communication between network participants. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014. [CrossRef]

62. Lee, Y.W.; Lee, Y.G. FTTH network survivability security based on massive fiber optic mechanical switch in consolidated central office. In Proceedings of the Digest of the 9th International Conference on Optical Internet (COIN), Jeju, Korea, 11–14 July 2010. [CrossRef]

63. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man in the Middle Attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*. [CrossRef]

64. Karakoc, E.; Dikbiyik, F. Rapid migration of VMs on a datacenter under cyber attack over optical infrastructure. In Proceedings of the 2016 HONET-ICT, Nicosia, Cyprus, 13–14 October 2016. [CrossRef]

65. Heo, Y.; Na, J. Development of unidirectional security gateway appliance using intel 82580EB NIC interface. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea; 19–21 October 2016. [CrossRef]

66. Reddi, R.M.; Srivastava, A.K. Real time test bed development for power system operation, control and cyber security. In Proceedings of the North American Power Symposium, Arlington, TX, USA, 26–28 September 2010. [CrossRef]

67. Stefanov, A.; Liu, C. Cyber-power system security in a smart grid environment. In Proceedings of the IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012. [CrossRef]

68. Hadbah, A.; Kalam, A.; Zayegh, Z. Powerful IEDs, ethernet networks and their effects on IEC 61850-based electric power utilities security. In Proceedings of the Australasian Universities Power Engineering Conference (AUPEC), Melbourne, VIC, Australia, 19–22 November 2017. [CrossRef]

69. Al-Salloum, Z.S.; Wolthusen, S.D. A link-layer-based self-replicating vulnerability discovery agent. In Proceedings of the IEEE symposium on Computers and Communications, Riccione, Italy, 22–25 June 2010. [CrossRef]

70. Sharma, G.; Pandey, N.; Hussain, I.; Kathri, S.K. Design of framework and analysis of Internet of things at data link layer. In Proceedings of the 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, India, 10–11 August 2017. [CrossRef]

71. Cioraca, A.; Voloh, I.; Adamiak, M. What protection engineers need to know about networking. In Proceedings of the 68th Annual Conference for Protective Relay Engineers, College Station, TX, USA, 30 March–2 April 2015. [CrossRef]

72. Tu, K. Communications Link Layer Security. In Proceedings of the International Conference on Communication Technology, Guilin, China, 27–30 November 2006. [CrossRef]

73. Lu, Z.; Shakeri, A.; Razo, M.; Tacca, M.; Fumagalli, A.; Galimberti, G.M.; Martinelli, G.; Swallow, G. Orchestration of reliable three-layer networks. In Proceedings of the 19th International Conference on Transparent Optical Networks (ICTON), Girona, Spain, 2–6 July 2017. [CrossRef]

74. Gerisch, A.; Lawniczak, A.T.; Di-Stefano, B. Building blocks of a simulation environment of the OSI network layer of packet-switching networks. In Proceedings of the CCECE 2003–Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology. Montreal, QC, Canada, 4–7 May 2003. [CrossRef]

75. Embry, J.; Manson, P.; Milham, D. An open network management architecture: OSI/NM Forum architecture and concepts. *IEEE Netw.* **1990**, *4*, 14–22. [CrossRef]

76. Li, Y.; Li, D.; Cui, W.; Zhang, R. Research based on OSI model. In Proceedings of the IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011. [CrossRef]

77. Wilder, R. Fairness issues for mixed TCP/OSI internets. In Proceedings of the MILCOM 91—Conference Record, McLean, VA, USA, 4–7 November 1991. [CrossRef]

78. Wang, Y.; Xiang, C. IP network-based trust management system. In Proceedings of the Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Shanghai, China, 26–28 July 2011. [CrossRef]

79. Zdrnja, B. Malicious JavaScript Insertion through ARP Poisoning Attacks. *IEEE Secur. Priv.* **2009**, *7*. [CrossRef]

80. Mirkovic, J.; Kissel, E. Comparative Evaluation of Spoofing Defenses. *IEEE Trans. Dependable Secur. Comput.* **2009**, *8*. [CrossRef]

81. Gupta, N.; Jain, A.; Saini, P.; Gupta, V. DDoS attack algorithm using ICMP flood. In Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016.

82. Raman, L.G. OSI upper layer protocol requirements for TMN operations. In Proceedings of the IEEE INFOCOM'88, Seventh Annual Joint Conference of the IEEE Computer and Communcations Societies. Networks: Evolution or Revolution? New Orleans, LA, USA, 27–31 March 1988. [CrossRef]

83. Silva, S.D. Transport Level Address for application level communication. In Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, 8–11 August 2009. [CrossRef]

84. Malhotra, A.; Sharma, V.; Gandhi, P.; Purohit, N. UDP based chat application. In Proceedings of the 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16–18 April 2010. [CrossRef]

85. Cai, L.; Pan, Y.; Guo, Y. Research on the effects of transport protocols on the application performance based on OPNET. In Proceedings of the IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, Japan, 26–29 June 2016. [CrossRef]

86. Pakanati, C.; Padmavathamma, M.; Reddy, N.R. Performance Comparison of TCP, UDP, and TFRC in Wired Networks. In Proceedings of the IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, India, 13–14 February 2015. [CrossRef]

87. Wang, S.; Xu, D.; Yan, S. Analysis and application of Wireshark in TCP/IP protocol teaching. In Proceedings of the International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT), Shenzhen, China, 17–18 April 2010. [CrossRef]

88. Xiao, S.; Deng, L.; Li, S.; Wang, X. Integrated TCP/IP protocol software testing for vulnerability detection. In Proceedings of the International Conference on Computer Networks and Mobile Computing, Shanghai, China, 20–23 October 2003. [CrossRef]

89. Weerathunga, P.E.; Cioraca, A. The importance of testing Smart Grid IEDs against security vulnerabilities. In Proceedings of the 69th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 4–7 April 2016. [CrossRef]

90. Jiwen, C.; Shanmei, L. Cyber security vulnerability assessment for Smart substations. In Proceedings of the IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Xi'an, China, 25–28 October 2016. [CrossRef]

91. Wang, Y.; Gamage, T.T.; Hauser, C.H. Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication. *IEEE Trans. Smart Grid* **2016**, *7*. [CrossRef]

92. Hung, T.C.; Khanh, T.P. Analyze and Evaluate the performance of SCTP at transport layer. In Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 7–10 February 2010.

93. Ramnath, D.; Deepak, T.; Krishnakumar, K.; Vijayaraghavan, S.; Ramanathan, R. An improved secret key update for multiple intersymbol obfuscation in physical layer security. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017. [CrossRef]

94. Yan, J.; Liu, C.; Govindarasu, M. Cyber intrusion of wind farm SCADA system and its impact analysis. In Proceedings of the IEEE/PES Power Systems Conference and Exposition, Phoenix, AZ, USA, 20–23 March 2011. [CrossRef]

95.　Aryai, S.; Binu, G.S. Cross layer approach for detection and prevention of Sinkhole Attack using a mobile agent. In Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 19–20 October 2017. [CrossRef]

96.　Kartalopoulos, S.V. Quantum Cryptography For Secure Optical Networks. In Proceedings of the IEEE International Conference on Communications, Glasgow, Scotland, 24–28 June 2007. [CrossRef]

97.　Guruprasad, A.; Pandey, P.; Prashant, B. Security features in Ethernet switches for access networks. In Proceedings of the TENCON 2003 Conference on Convergent Technologies for Asia-Pacific Region, Bangalore, India, 15–17 October 2003. [CrossRef]

98.　IEEE. *802.1AEcg-2017—IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 3: Ethernet Data Encryption Devices*; IEEE Standards Document; IEEE: Piscataway, NJ, USA, 2017. [CrossRef]

99.　Witzke, E.L.; Gossage, S.; Wiener, D.J. An Architecture for Multi-Security Level Network Traffic. In Proceedings of the 40th Annual 2006 International Carnahan Conference on Security Technology, Lexington, KY, USA, 16–19 October 2006. [CrossRef]

100.　Wahid, K.F. Maximizing Ethernet Security by Switch-Based Single Secure Domain. In Proceedings of the Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 12–14 April 2010. [CrossRef]

101.　Su, S.; Duan, X.; Zeng, X.; Chan, W.L.; Li, K.K. Context Information based Cyber Security Defense of Protection System. In Proceedings of the IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 24–28 June 2007. [CrossRef]

102.　Penera, E.; Chasaki, D. Packet scheduling attacks on shipboard networked control systems. In Proceedings of the 2015 Resilience Week, Philadelphia, PA, USA, 18–20 August 2015. [CrossRef]

103.　Kirkpatrick, M.E. A security standard for LANs. In Proceedings of the Fifth Annual Computer Security Applications Conference, Tucson, AZ, USA, 4–8 December 1989. [CrossRef]

104.　Kiravuo, T.; Sarela, M.; Manner, J. A Survey of Ethernet LAN Security. *IEEE Commun. Surv. Tutor.* **2013**, *15*. [CrossRef]

105.　Hadjina, N.; Thompson, P. Data security on Ethernet LANs. In Proceedings of the 10th Mediterranean Electrotechnical Conference. Information Technology and Electrotechnology for the Mediterranean Countries. Proceedings. MeleCon, 2000 (Cat. No.00CH37099), Lemesos, Cyprus, 29–31 May 2000. [CrossRef]

106.　Yeung, K.H.; Yan, F.; Leung, C. Improving Network Infrastructure Security by Partitioning Networks Running Spanning Tree Protocol. In Proceedings of the International Conference on Internet Surveillance and Protection, Cote d'Azur, France, 26–29 August 2006. [CrossRef]

107.　Scott, B.; Xu, J.; Zhang, J.; Brown, A.; Clark, E.; Yuan, X. An interactive visualization tool for teaching ARP spoofing attack. In Proceedings of the IEEE Frontiers in Education Conference (FIE), Indianapolis, IN, USA, 18–21 October 2017. [CrossRef]

108.　Meghana, J.S.; Subashri, T.; Vimal, K.R. A survey on ARP cache poisoning and techniques for detection and mitigation. In Proceedings of the Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 16–18 March 2017. [CrossRef]

109.　Bhirud, S.G.; Katkar, V. Light weight approach for IP-ARP spoofing detection and prevention. In Proceedings of the Second Asian Himalayas International Conference on Internet (AH-ICI), Kathmandu, Nepal, 4–6 November 2011. [CrossRef]

110.　Nelson, R. End-to-end encryption at the network layer. In Proceedings of the Fifth Annual Computer Security Applications Conference, Tucson, AZ, USA, 4–8 December 1989. [CrossRef]

111.　Sanaiye, O.A. Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. In Proceedings of the 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015. [CrossRef]

112.　Duan, Z.; Yuan, X.; Chandrashekar, J. Controlling IP Spoofing through Interdomain Packet Filters. *IEEE Trans. Dependable Secur. Comput.* **2007**, *5*. [CrossRef]

113.　Chuiyi, X.; Yizhi, Z.; Yuan, B.; Shuoshan, L.; Qin, X. A Distributed Intrusion Detection System against flooding Denial of Services attacks. In Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011), Seoul, Korea, 13–16 February 2011 .

114. Udhayan, J.; Anitha, R. Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis. In Proceedings of the IEEE International Advance Computing Conference, Patiala, India, 6–7 March 2009.

115. Blackridge. BlackRidge TAC Gateways: Quick Start Guide. In *BlackRidge Technology User Guide*; BlackRidge Technology Inc.: Reno, NV, USA, 2016.

116. Logeshwari, K.; Lakshmanan, L. Authenticated anonymous secure on demand routing protocol in VANET (Vehicular adhoc network). In Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 23–24 February 2017. [CrossRef]

117. Sirohi, P.; Agarwal, A.; Tyagi, S. A comprehensive study on security attacks on SSL/TLS protocol. In Proceedings of the 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 14–16 October 2016. [CrossRef]

118. Dong, K.; Yang, S.; Wang, S. Analysis of low-rate TCP DoS attack against FAST TCP. In Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications, Jinan, China, 16–18 October 2006. [CrossRef]

119. Kolahi, S.S.; Treseangrat, K.; Sarrafpour, B. Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13. In Proceedings of the International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15), Sharjah, UAE, 17–19 February 2015. [CrossRef]

120. Chen, Z.; Wen, W.; Yu, D. Detecting SIP flooding attacks on IP Multimedia Subsystem (IMS). In Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 30 January–2 February 2012. [CrossRef]

121. Narayan, S.; Gupta, R.; Kumar, A.; Ishrar, S.; Khan, Z. Cyber security attacks on network with transition mechanisms. In Proceedings of the International Conference on Computing and Network Communications (CoCoNet), Trivandrum, India, 16–19 December 2015. [CrossRef]

122. Wang, H.-Y.; Cao, H.-Z.; Zhu, X.; Ji, C.-J.; Ji, X.-J. The Security and Promotion Method of Transport Layer of TCP/IP Agreement. In Proceedings of the Second International Conference on Information Technology and Computer Science, Kiev, Ukraine, 24–25 July 2010. [CrossRef]

123. Al-Jarrah, M.; Tamimi, A.R. A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement. In Proceedings of the Innovations in Information Technology, Dubai, UAE, 19–21 November 2006. [CrossRef]

124. Chang, R.K.C.; Fung, K.P. Transport layer proxy for stateful UDP packet filtering. In Proceedings of the ISCC 2002 Seventh International Symposium on Computers and Communications, Taormina-Giardini Naxos, Italy, 1–4 July 2002. [CrossRef]

125. Chang, B.; Liang, Y.; Jin, J. Adaptive cross-layer-based TCP congestion control for 4G wireless mobile cloud access. In Proceedings of the IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Nantou, Taiwan, 27–29 May 2016. [CrossRef]

126. Carter, C.; Onunkwo, I.; Cordeiro, P.; Johnson, J. Cyber Security Assessment of Distributed Energy Resources. In Proceedings of the IEEE Photovoltaic Specialists Conference (PVSC), Washington, DC, USA, 25–30 June 2017.

127. Castiglione, A.; D'Arco, P.; Santis, A.D.; Russo, R. Secure group communication schemes for dynamic heterogeneous distributed computing. *Future Gener. Comput. Syst.* **2017**, *74*, 313–324. [CrossRef]

128. GWAC. *GridWise Interoperability Context-Setting Framework*; GridWise Architecture Council (GWAC) Technical Report; GridWise Architecture Council (GWAC): Richland, WA, USA, 2008.

129. NIST. *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0.*; National Institute of Standards & Technology Technical Report; NIST: Gaithersburg, MD, USA, 2010.