Dijlah Journal of Engineering Sciences (DJES) **Vol. 1, No. 3, December, 2024, pp. 99-107**
ISSN: Printed: 3078-9656, Online: 3078-9664, paper ID: 19

The Interconnection of Open Systems Resolution of OSI Levels and the Dilemma of Discrete Energy in Security and Legal

Nazar Jabbar Alhyani[1], Oday Kamil Hamid[2] , Ali Mohammed Kadhim[3] ,
[1, 2, 3]Department of Computer Techniques Engineering, Dijlah University College, Iraq

oday.kamil@duc.edu.iq

Article Info

Article history:

Received Oct. 15,2024
Revised Nov. 10, 2024
Accepted Dec. 1, 2024

Keywords:

OSI Level
Resolution
Challenge
Resource Security

ABSTRACT

The incorporation of technology into our everyday lives and medium-sized corporations has become obvious, as most businesses cannot operate without the use of technology. This has resulted in weaknesses and shortcomings in security. The layered protocol model of Open System Interconnection (OSI) divides networking duties into layers and specifies a collection of offerings for each component to be offered separately. The protocol's design allows services to be realized for various levels; however, no direct communication between nonadjacent layers is allowed because the architecture prohibits such an action; communication is also restricted to carrying out calls and replies between adjacent layers. The smart grid's expansion of distributed energy resources is increasing, causing solar distribution to extend network attack surfaces. As a result, there is a mismatch between implementation and adequate knowledge of security in communication needs. Nowadays, the literature lacks protocol level susceptibility, solution map, and assaults to all layers in the logic model, as in Open Systems Interconnection (OSI) stacks inside vendors sporting proprietary approaches to mitigate attack host. This paper examines the primary vulnerability, viable remedy, and attack level of wind and solar protocol. As a result, our study provides a starting point for vendors, utilities, aggregators, and new manufacturing investors to develop a basic understanding of the safety problem, which is a prerequisite for understanding securities requirements.

Corresponding Author:

Oday Kamil Hamid
Department of Computer Engineering Techniques,
Dijlah University College, Iraq, Baghdad.
Email: oday.kamil@duc.edu.iq

1. INTRODUCTION

The incorporation of distributed energy resources (DER) such as solar and wind into smart grids is presently increasing. This device is outfitted with actuating and sensing devices such as a smart inverter, data collection controller, and phasor measuring unit with metering structure. The device multiplicity utilizes several communication systems with media to communicate data to utility instructions and the command- and control center through a control signal of gotten waveforms.

The Open System Interconnection (OSI) layered protocol model divides networking duties into layers and defines a collection of services for each component to be provided separately. Asdaque proposed a cross-layer design that deviates from the reference architecture by permitting direct contact between protocols on different levels. It also allows variables to be shared between levels, which increases wireless transmission effectiveness [1].

Ajala and Thaier illustrate the integration, execution, and arrangement of secure communication links between business spread while considering a flexible multipoint virtual private network and maintaining the previously mentioned link to IP security in order to secure corporate business networks [2].

In order to safeguard OSI, Ramtin and Uzzam also stated the physical layer. They investigated whether independent wireless carriers can effectively collaborate using software-defined wireless networking to achieve secret wireless interactions and optimise useable performance in a highly saturated frequency while maintaining physical-layer security-allowed secrecy [3]. Because of their restricted computational processing capacity, fifth-generation (5G) and beyond fifth-generation (B5G) cellular networks are vulnerable to spying attacks. In a scenario involving two people operating over fading channels, the concealment performance of Adrián and Brandon's proposed power-domain non-orthogonal multiple-access systems affected by imprecise sequential interference cancellation is evaluated [4].

In the Internet of Things, wireless sensor networks (WSN) serve a key role in improving the general flexibility of industrial resources and thus boosting effectiveness. (IoT). Muhammad and Zurina propose efficient data link layer security algorithms for WSN and IoT-based systems [5].

In contrast to a grid that only uses the cloud, fog computing uses both clouds and end devices to collect, process, and act on data locally at the edge for low-latency applications before sending it to the cloud for more complex operations. It also offers enhanced efficiency and seamless integration, better scalability, visibility, and greater availability. Fog computing on smart grid systems is a suggestion made by Anzalchi [6].

The rising ubiquity of sensing and communication acting, matching susceptibility that might propose that climbing [6-8]. The vendor's deployment of numerous tiers of protection through proprietary approaches [9-12] demonstrates the absence of security needs for DER in the present and emerging situation. Mission impact analysis (MIA) aims to make it easier to combine military or commercial operations with cyber protection. The MIA model was created by Alexander Kott, who also created methods for building and validating models that are affordable [10]. As a consequence, remote DER's commitment to standards and interoperable concerns that now impact consumers has little to no truth. Usingtruerd-party vendor for monitoring and analytic visualization, which relies on a communications connection with no encrypted security safeguards [13-18] several drawbacks of current methods to DER security, such as the smart inverter, were uncovered and presented via multiple interviews with large utilities. When there is a high degree of vulnerability, there is no encrypting of communication from the switchgear to the control center, which is often focused on servicing security shortcomings [19-21]. This book contains substring contributions such as the present literature's flaws and tries to bridge the gap between an extensive study, assaults, and remedies. Furthermore, this study gives roadmaps to assure successful DER security via suggested compliance papers that include the most fundamental features of safe control. Such documentation might accompany certain IEEE and other organizations' development standards to secure DER information and the communications substructure. The rounded intangible distributions of astute grids in communication design that include all devices from the grid's edges to control and directives are distinctive of the inadequate work. This conventional and well-understood map of protocol requirements on communications controller’s protocols and internet protocols (TCP/IP) substrates to exposed system interconnected (OSI) essential references. This will act as a single point of reference for industry and research members in the connected subject. It formerly contributed significantly to the literature gap by giving thorough documentation to the sectors and gathering all DER weaknesses for wind turbines and PV. The identification of holes in DER communication security needs the accomplishment to provide a defensive layer model capable of resolving the identified gaps. The flow chart in Figure 1 summarizes the effort.

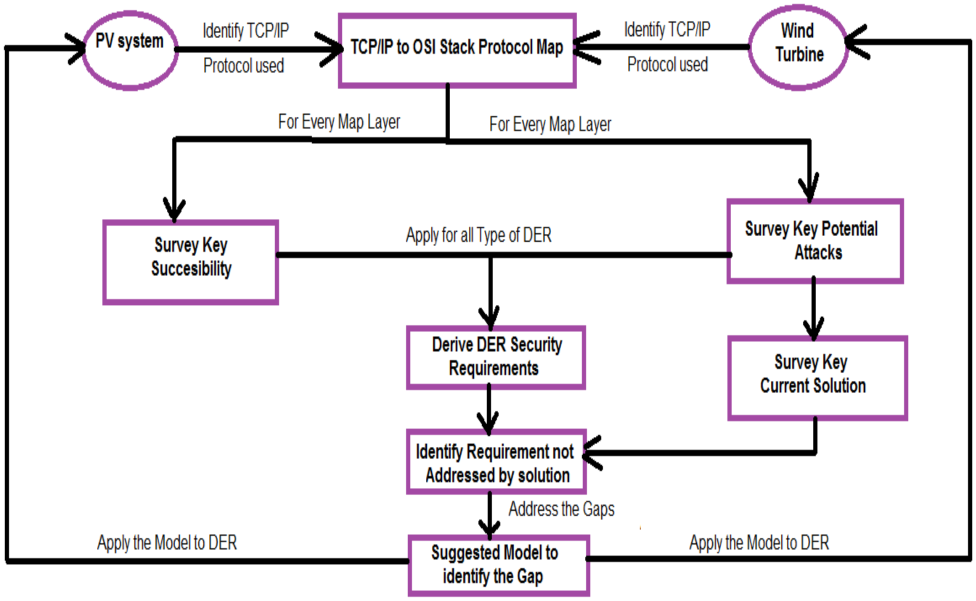

PV system
Identify TCP/IP
Protocol used
TCP/IP to OSI Stack Protocol Map
Identify TCP/IP
Protocol used
Wind Turbine
For Every Map Layer
For Every Map Layer
Survey Key Succesibility
Apply for all Type of DER
Survey Key Potential Attacks
Derive DER Security Requirements
Survey Key Current Solution
Identify Requirement not Addressed by solution
Address the Gaps
Apply the Model to DER
Suggested Model to identify the Gap
Apply the Model to DER

Figure 1: Flow Sequence of Research Efforts

Wind turbines and PV are only included in DER approaches, and their privacy must be respected in the distribution field per NIST's smart grid design. The phases of the sequence of activities, methods, or techniques of TCP/IP frameworks and DER interact with different protocols and devices at each layer to collect all protocols. Since the architectural model is well known, mappings between the OSI layer and recognized protocols are conducted for more extensive inspections. The DER is assumed to prevent these assaults at all commons that depend on protocols, regardless of their kind, attacks, flaws, or remedies. As a consequence, the collective examines all layers of threats and vulnerabilities, resulting in synthesis to drive the various wind DER and PV security standards that negate the solution that should fulfill them. To demonstrate how these gaps can be filled, an analysis of existing solutions that meet all criteria, as well as the disparity in these systems' competencies, is conducted. In addition, to meet the unmet security need, the design approval process through the test case is performed for the recommended model. The OSI acronym stands for open system interconnections, which was developed by international organizations in 1980 [7, 18]. The architecture of this system is made up of seven levels, each of which performs a distinct role. As shown in Figure 2, these layers collaborate to convey information from one individual to another through globality [22-25].

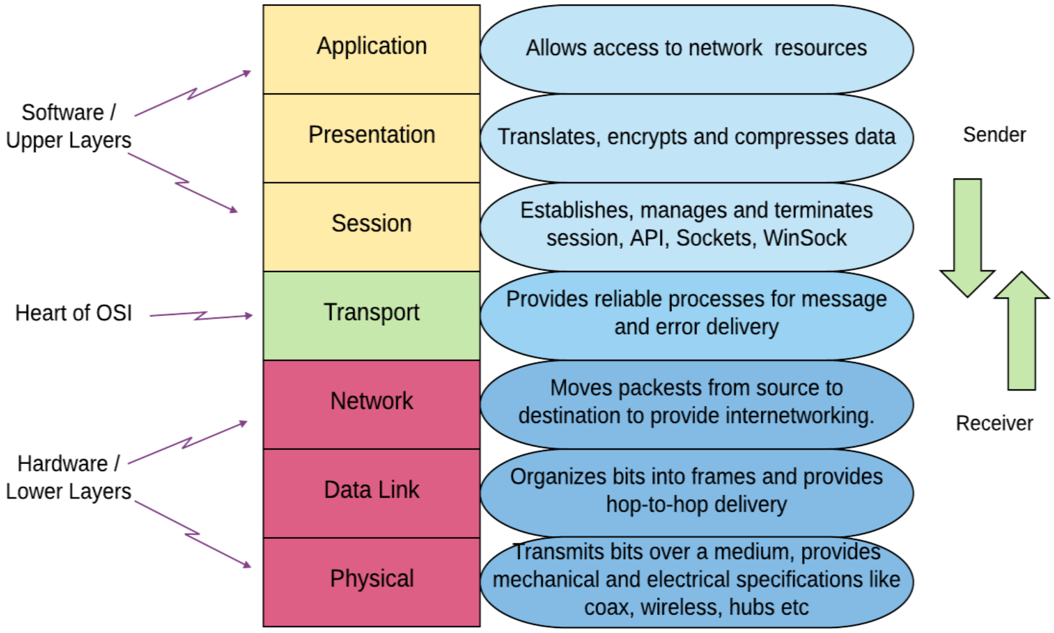
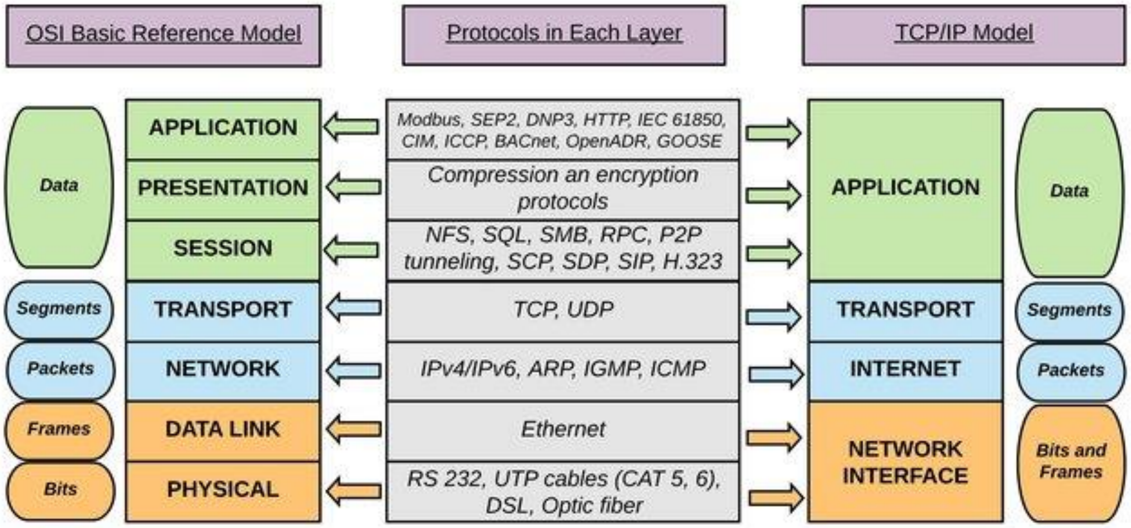

Application
Allows access to network resources
Software / Upper Layers
Presentation
Translates, encrypts and compresses data
Sender
Session
Establishes, manages and terminates session, API, Sockets, WinSock
Heart of OSI
Transport
Provides reliable processes for message and error delivery
Network
Moves packests from source to destination to provide internetworking.
Receiver
Hardware / Lower Layers
Data Link
Organizes bits into frames and provides hop-to-hop delivery
Physical
Transmits bits over a medium, provides mechanical and electrical specifications like coax, wireless, hubs etc

Figure 2: Network OSI Model Layers Explained

This study examines the first four OSI layers, which are physical, transportation, networks, and information linkages. Additional layers, such as further synthesis, are planned for future study when this idea is completed. Part two is in the works, and will include the decision of co-decision substructure using the e in wind and PV distribution with authorities, as well as the routing protocol map between the OSI and TCP/IP models. Part 3 is an overview of the key flaws of DER communication methods. Section 4 depicts the possible cyberattack caused by productive maltreatment. Section 5 includes the conclusion of the paper.

2. MATERIALS And PROCEDURES

DER and PV communication substructures are being investigated for interoperability.
With effectiveness CCC in the communications network and the primary susceptibilities being discrete and abbreviated. As a practical implementation of current theories known as OSI reference models, the most current smart grid device communication utilizes an avionics layer protocol that runs on TCP/IP stacks. As shown in Figure 3, the linkage seen between the OSI model and the TCP/IP stack must be grasped further to understand how these protocols function.

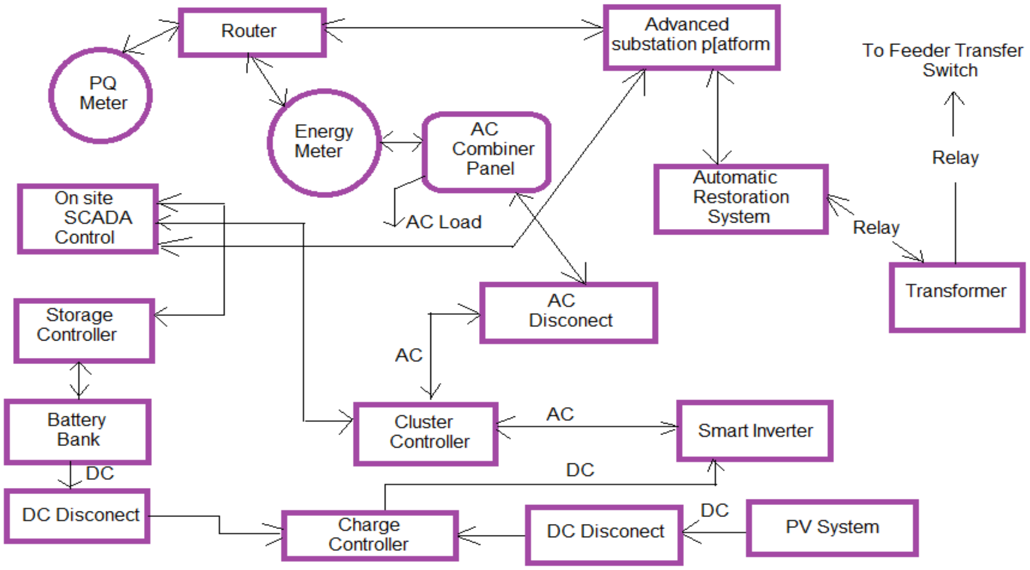


	OSI Basic Reference Model	Protocols in Each Layer	TCP/IP Model	
Data	APPLICATION	Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE	APPLICATION	Data
	PRESENTATION	Compression an encryption protocols		
	SESSION	NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323		
Segments	TRANSPORT	TCP, UDP	TRANSPORT	Segments
Packets	NETWORK	IPv4/IPv6, ARP, IGMP, ICMP	INTERNET	Packets
Frames	DATA LINK	Ethernet	NETWORK INTERFACE	Bits and Frames
Bits	PHYSICAL	RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber		

Figure 3. The map between TCP/IP stacks with OSI rudimentary reference prototypical

TCP/IP stacks are acknowledged as a metamodel for network connection for all purposes in the OSI model, and they are more effective in abstracting communications. The development of the internet is mostly focused on linking devices and TCP/IP stacks for point-to-point communication. compare-user user applications, data must be formatted, fragmented, coded, decoded, packed, sent, and received. As a result, the previous OSI model is inflexible in terms of the established levels and is inapplicable to the internet's network. In addition to the physical layer in OSI models, the network interface layers in TCP/IP stacks correspond to the data link. The internet layers, like the OSI network levels, perform responsibilities that are eclipsed by the transport layers allocated to each tour to make a connection, construct an interface, and preserve context with any application, the OSI model divides the presentation, session, and application layers. These services merge the TCP/IP stacks into a single layer called "implementation" in both the TCP/IP and OSI models, which are explored under security. Corporeal security devices with broadcasting admission limits may filter the network border layers as well as the duplicated private network at internet levels hidden by security socket layers. Finally, there are hosted firewall and proxy layers. These levels of security are insufficient to withstand sophisticated attacks on humans or the emerging persistent danger. This research recently provided a paradigm for security in TCP/IP stacks by examining the usage of 512-bit block ciphering and increasing internet-controlling message protocols by leveraging vacant bits in the validation portions of ICMP packets. The physical layer of OSI models protects network equipment against physical attacks such as fire, cutting, manipulation, water, and signal disruption caused by interference. Backup and restore and role-based access control are two for assuring layer security, and the data connection layers are prone to tree attacks. In the transport layer and network, technologies such as intrusion prevention systems (IPS), intrusion detection systems (IDS), swaps, and access restrictions were utilized to mitigate assaults such as denial of service and unauthorized access. The primary threats to the presentation and session levels are account access and unauthorized data, which may be managed by authentication and encryption techniques. The application layer attack included but was not limited to, malware entrance and exploit malicious code and social engineering inoculation. A complexity-based security solution may mitigate this attack to some extent, but it might be significantly enhanced by upgrading the models using approaches such as regular version updates, limited backdoors, training, and awareness. Figures 4 and 5 demonstrate the distributed PV, which may interact with its effectiveness in a variety of ways. The arrangement is orthogonal, with a grid-edge device on the bottom and the CCC application on top. Dispersed PV devices include a smart inverter and a manufacturing meter that record the energy provided by the systems versus the haggard energies from grids at points of interaction or prevalent coherence, micro- or high-frequency disruptions, and plant-level control that communicates directly with SCADA. A contactor, capacitor bank, switch monitor, and load tap changer are examples of intelligent electronic devices that may vary in frequency and voltage.

Figure 4:



Distributed PV scheme

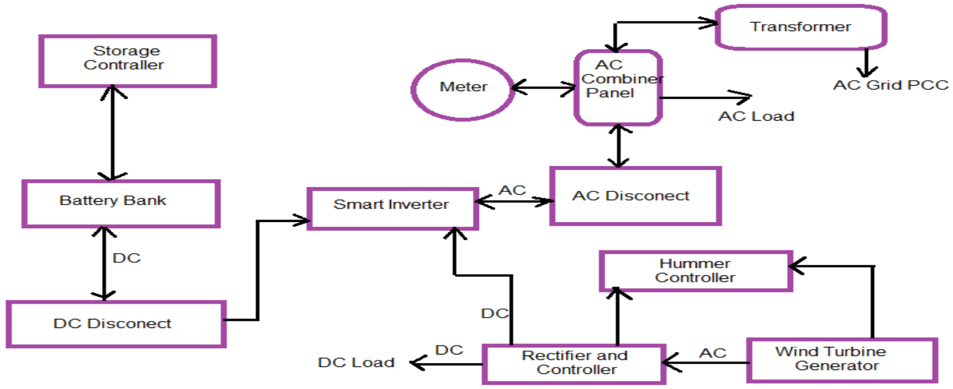


Figure 5: Distributed wind turbine scheme

For each layer of the manifolds protocol, different protocols are used at multiple spatial levels. The semantic and economic backdrop layers of the GWAC interoperable stacks extend the grid-wise susceptibility study and the OSI architecture by seven levels. The major qualities of each layer are summarized in Table 1.

Table 1. DER Communications-Levels Susceptibilities Layer

Layers	The number of layers	Protocol	Smart Grids layer	Standards	Susceptibilities
Physical	1	UTP, DSL, RS 232, Optic fibers	Network, Edges, Fields	Hardware	Hardware's theft, data, wiretap
Data link	2	Ethernet	Fields, Edges	IEEE 802.1 IEEE 802.3	VLAN, remote access, control, switching
Network	3	ARP, IPv4, IPv6, ICMP	Fields, Edge	IETF	TCP Sequencsessionssion,
Transport	4	UDP, TCP	All	DARPA, IETF	TCP Sequence, port scan

Table 2 provides a quick overview of existing prevention techniques for different assaults that may leverage these vulnerabilities.

Table 2. Communication-Level Attack and Current Solution Layer

Layers	The number of layers	Protocol	Potential Attack	Current solution
Physical	1	UTP, DSL, RS 232, Optic fibers	Data slurp, steal data, wiretap, physical asset, obstruction	USB block, cryptography of data storage
Data link	2	Ethernet	Field, Edge	Network segmentation, physical protection, port security
Network	3	ARP, IPv4, IPv6, ICMP	Field, Edge	Packet filter, firewall, proxy
Transport	4	UDP, TCP	All	ARP modifying, IP addressed authenticated

3. RESULTS AND DISCUSSION

The inadequate at assault has been experienced at every layer, as demonstrated by several incidents in the literature, such as the MAC flood that attacked any device in DER contexts. Authentication of access points and user ethernet in the data link layers, such as control schemes, switches and routers, smart meters, and synchrophasors in the organization of contributory infringement, the most effective current methods that have been advocated by industries to combat natural assaults are unoccupied port security and predefining the MAC address numbers on specified switch ports. An attacker may frequently improve unwanted network access on the IP address monitored device by modifying the header information of the IP address providers. It is now advised that the router's IP filter be used to map the income traffic interfaces to the design interface of IP address sources given in the MAC address table above. Rahim, on the other hand, introduced cross-layer design to allow for the coordination, interaction, and joint optimization of protocols traversing several layers in addition to maintaining the characteristics related to the original layers [1]. [3] Recommended using wireless networking's physical-layer-based software to implement secure communication over wireless networks. Many intrusion detection inline block tools and prevention systems are capable of detecting malicious ARP packets to guarantee the reliability and integrity of MAC addresses. Packets in the DER device repeat the standard observe attack, where the set points command is combined with other changes requested for originality from the client application via UDP or TCP cloud, which may intercept and alter. Because these requests and directives must be unencrypted to be realistic, this assault is dominant. This effort is being carried out completely by the federal alternative fuels greenroom, which conducted the survey, collated the data, and produced the papers. In addition. The Operational Coalition for Renewable Energy improved and wrote this work.

The viewpoint represented in this report does not necessarily reflect the viewpoint of DOE, although only limited efforts for guidance and mentoring were sponsored locally via grants.

The lowest-level protocol scrap metal in DER categories runs on TCP/IP stacks and has been transferred from these stacks to OSI models, leading to a new theoretical security concern and a solution.

4. CONCLUSION

This article describes the existing structure of DER authentication and encryption at distributing smart grid levels, with an emphasis on OSI layers four through eight. In DER domains, the lowest-level protocol castoff runs on TCP/IP stacks and has been translated from these stacks to OSI models, resulting in a fresh theoretical security problem along with a solution. Depending on the evaluation, the highest-level summary of various advanced security control requirements drives to ensure that DER communication and information security has been properly examined and discussed. The current system has conflicting needs for executing inadequate gains and social engineer assaults, which leverage technological weaknesses and anthropomorphic faintness to identify and respond to these attacks on layers 1-4. More study is required in the future to fine-tune this model, which will raise the protocol's sensitivity to assaults and potential attacks in the existing OSI layer solution.

REFERENCES

[1] A. Rahim, "Cross Layer Design and Energy Efficient Protocol for Wireless Sensor Network," *Applied Science and Engineering Journal for Advanced Research,* vol. 2, no. 1, pp. 8-12, 2023.

[2] A. Ajala and T. Hamid, "Network Security and Management of Medium Enterprise Business Network," EasyChair, 2516-2314, 2023.

[3] R. Ranji, U. Javed, B. Boltjes, F. Bouhafs, and F. Den Hartog, "Optimizing wireless network throughput under the condition of Physical Layer Security using Software-Defined Networking enabled collaboration," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 2023: IEEE, pp. 1-6.

[4] A. S. Arias, L. C. Huera, B. S. Rueda, H. R. Carvajal, N. V. Orozco, and F. D. Almeida, "On the Secrecy Outage Probability of NOMA Systems Affected by Imperfect SIC over κ− μ Fading Channels," *Journal of Communications,* vol. 18, no. 3, 2023.

[5] M. Z. Hasan and Z. Mohd Hanapi, "Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review," *Electronics,* vol. 12, no. 2, p. 458, 2023.

[6] A. Anzalchi, A. Sundararajan, L. Wei, A. Moghadasi, and A. Sarwat, "Future directions to the application of distributed fog computing in smart grid systems," in *Cloud Security: Concepts, Methodologies, Tools, and Applications*: IGI Global, 2019, pp. 2186-2212.

[7] A. Sundararajan, T. Khan, H. Aburub, A. I. Sarwat, and S. Rahman, "A tri-modular human-on-the-loop framework for intelligent smart grid cyber-attack visualization," in *SoutheastCon 2018*, 2018: IEEE, pp. 1-8.

[8] L. Wei, A. H. Moghadasi, A. Sundararajan, and A. I. Sarwat, "Defending mechanisms for protecting power systems against intelligent attacks," in *2015 10th System of Systems Engineering Conference (SoSE)*, 2015: IEEE, pp. 12-17.

[9] J. S. Meghana, T. Subashri, and K. Vimal, "A survey on ARP cache poisoning and techniques for detection and mitigation," in *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, 2017: IEEE, pp. 1-6.

[10] A. Kott, M. Lange, and J. Ludwig, "Approaches to modeling the impact of cyber attacks on a mission," *arXiv preprint arXiv:1710.04148,* 2017.

[11] E. Ibrahim, "A cyber security solutionurity," *National Renewable Energy Laboratory (NREL) Technical Paper*, 2017.

[12] E. Ibrahim, "Disruptive ideas for power grid security and resilience with der," National Renewable Energy Lab.(NREL), Golden, CO (United States), 2017.

[13] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols," in *2017 8th International conference on information technology (ICIT)*, 2017: IEEE, pp. 685-690.

[14] A. I. Sarwat, A. Sundararajan, and I. Parvez, "Trends and future directions of research for smart grid IoT sensor networks," in *International Symposium on Sensor Networks, Systems and Security,* 2017: Springer, pp. 45-61.

[15] K. SunilKumar, "A review on security and privacy issues in wireless sensor networks," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017: IEEE, pp. 1979-1984.

[16] S. S. Hussain, T. S. Ustun, P. Nsonga, and I. Ali, "IEEE 1609 WAVE and IEC 61850 stacommunication-based integrated EV charging management in smart grids," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7690-7697, 2018.

[17] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, p. 2360, 2018.

[18] A. S. Alazri, "Telecommunication traffic through submarine cables: Security and vulnerabilities," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016: IEEE, pp. 372-375.

[19] E. Karakoc and F. Dikbiyik, "Rapid migration of VMs on a datacenter under cyber attack over optical infrastructure," in *2016 HONET-ICT*, 2016: IEEE, pp. 54-58.

[20] Y. Heo and J. Na, "Development of unidirectional security gateway appliance using intel 82580EB NIC interface," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, 2016: IEEE, pp. 1194-1196.

[21] B. Scott *et al.*, "An interactive visualization tool for teaching ARP spoofing attack," in *2017 IEEE Frontiers in Education Conference (FIE)*, 2017: IEEE, pp. 1-5.

[22] K. Logeshwari and L. Lakshmanan, "Authenticated anonymous secure on-demand routing protocol in VANET (Vehicular ad-hoc network)," in *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, 2017: IEEE, pp. 1-7.

[23] P. Sirohi, A. Agarwal, and S. Tyagi, "A comprehensive study on security attacks on SSL/TLS protocol," in *2016 2nd international conference on next generation computing technologies (NGCT)*, 2016: IEEE, pp. 893-898.

[24] C. Lai *et al.*, "Cyber security primer for DER vendors, aggregators, and grid operators," *Tech. Rep.*, vol. 12, 2017.

[25] A. Castiglione, P. D'Arco, A. De Santis, and R. Russo, "Secure group communication schemes for dynamic heterogeneous distributed computing," *Future Generation Computer Systems*, vol. 74, pp. 313-324, 2017.

BIOGRAPHIES OF AUTHORS

	Nazar Jabbar Alhyani Received his Ph.D. of Science in Electronic Engineering from the University of Buckingham - UK in 2015. Currently, he is a university staff at Dijlah University College Iraq (DUC). His research interests include secure transmission, video encryption and compression, cloud security, and data encryption.
	Oday Kamil Hamid Received his Bsc. in Electrical Engineering and Msc. Degree in Communication Engineering from the University of Technology Iraq in 2000 and 2003 respectively. Currently, he is a senior lecturer in the Faculty of Computer Engineering Techniques at Dijlah University College Iraq (DUC). His research interest, are communication, security, digital signal processing, speech recognition, and neural network.
	Ali Mohammed Kadihm Received his Master of Computer Science information systems. Bachelor's degree / College of Science - University of Mosul 1982. Higher Diploma / UEA-England 1990. Master's degree/ University of Technology - Iraq.1992.

الخلاصة

لقد أصبح دمج التكنولوجيا في حياتنا اليومية والشركات المتوسطة الحجم واضحًا، حيث لا تستطيع معظم الشركات العمل بدون استخدام التكنولوجيا. وقد أدى هذا إلى نقاط ضعف ونواقص في الأمن. يقسم نموذج البروتوكول الطبقي لربط الأنظمة المفتوحة (OSI)مهام الشبكات إلى طبقات ويحدد مجموعة من العروض لكل مكون يتم تقديمها بشكل منفصل. يسمح تصميم البروتوكول بتحقيق الخدمات لمستويات مختلفة؛ ومع ذلك، لا يُسمح بالاتصال المباشر بين الطبقات غير المتجاورة لأن البنية تحظر مثل هذا الإجراء؛ كما يقتصر الاتصال على إجراء المكالمات والردود بين الطبقات المتجاورة. يتزايد توسع الشبكة الذكية لموارد الطاقة الموزعة، مما يتسبب في توسيع توزيع الطاقة الشمسية لأسطح الهجوم على الشبكة. ونتيجة لذلك، هناك عدم تطابق بين التنفيذ والمعرفة الكافية بالأمن في احتياجات الاتصالات. في الوقت الحاضر، تفتقر الأدبيات إلى قابلية مستوى البروتوكول وخريطة الحل والهجمات على جميع الطبقات في النموذج المنطقي، كما هو الحال في مجموعات ربط الأنظمة المفتوحة (OSI) داخل البائعين الذين يتبنون نهجًا خاصًا للتخفيف من المضيف الهجومي. تدرس هذه الورقة نقاط الضعف الأساسية والعلاج القابل للتطبيق ومستوى الهجوم في بروتوكولات الرياح والطاقة الشمسية. ونتيجة لهذا، توفر دراستنا نقطة انطلاق للبائعين وشركات المرافق والمجمعين والمستثمرين الجدد في التصنيع لتطوير فهم أساسي لمشكلة السلامة، وهو شرط أساسي لفهم متطلبات الأوراق المالية.