

# SDWSN: Software-Defined Wireless Sensor Network

Shanu Bhardwaj, S.N. Panda, Chih-Yung Chang

**Abstract:** Nowadays, several protocols and treaties coexist in the Internet world that dispenses the services to the users. But the distributed management and the control decisions make the network modest to control. Due to these problems, the behavior of the network becomes unpredictable and insufficient. Hence, there is a lack of flexibility in the conventional network architecture like in Wireless Sensor Network (WSN). Therefore, Software-Defined Networking (SDN) finds the deficiencies of the previous technologies and isolated both the planes named as control and data plane. It aims to make the network more simplified and flexible with respect to that of the traditional one. The SDN application in WSN is very commanding in terms of network configuration and network management, leading to an emerging network technology known as Software-Defined Wireless Sensor Network (SDWSN). Therefore, the paper presents the challenges in SDWSN in terms of the management and configuration of the network. The pitch is to comprehend the current challenges with an end goal to ensure more security, efficiency, and dependability. We reviewed several works of literature such as SDN, WSN, and SDWSN and present the findings in terms of architecture, challenges, and their solution. This paper shows how SDN is included in WSN to solve the existing challenges.

**Keywords:** SDN, WSN, Challenges, Security, Scalability, Network Management, Network Configuration, SDWSN.

## I. INTRODUCTION

In today's world, the networking shell is developing quickly. On one hand, the immense Internet Protocol (IP) network provides strong connectivity between the users but on the other hand, there is an existence of the network management issues due to expanding in the framework of the WSN [1]. Therefore, the IP network is becoming large and complex bit-by-bit. In the conventional network, the router contains both the planes: data as well as the control plane [2]. The control plane consists of a routing algorithm inside the router whereas the data plane, which is commonly known as the forwarding plane, used to forward/move the datum to the next-hop [3]. SDN addresses the weakness of the traditional technologies and performs accordingly, to carry the traffic in the upright destination in an automated way [4].

Communication technology has encountered a large progression since the 1980s to move towards becoming what is at present SDNs [5], [6]. SDN is a prominent networking

standard that expects to alter the constraints of traditional network infrastructures by carrying all the control functionalities to a centralized area [7]. SDN allows the isolation of data as well as the control plane, as a result, switches will become the forwarding/moving devices whereas the control plane works as the centralized controller [8].

WSN is the technology that gains popularity in recent years due to the cheap and the rapid development of the smart/automated sensors [9]. The primary stuff of the smart sensors in the sensor network is the cut-priced power utilization among all others, where the data have to be deployed [10]. In WSN topology, the sensors nodes run together from few to several thousand to collect the data packets from the surroundings [11]. The major applicability of WSN is sorted into two fine categories [12]:

- Tracking applications: Tracks the entities like vehicle, humans, animals and other objects.
- Monitoring applications: Monitors environmental scenarios.

As a result, taking all the prime characteristics of both the technologies: SDN and WSN, a new technology emerges called SDWSN [13]. SDWSN is based on nodes that are smart but also includes the programming capability of SDN [14]. Therefore, the new emerging technology SDWSN is flexible in terms of modifying their motivations into different applications. This paper furnishes a classification of some of the traditional wireless networks with the applications of SDN in them. Several SDN proposed solutions in WSN to improve the challenges are shown.

The remainder section of this paper is assembled as follows: Section II provides the similar work done in the field of SDN and WSN. Section III of the paper presents the introduction of SDN followed by the architecture of SDN. Section IV introduces WSN followed by an architecture of WSN. Section V discusses the SDWSN along with architecture, challenges and their solution. Finally, the paper concludes with the conclusion in this work.

## II. RELATED WORK DONE IN SDN AND WSN

The birthing of SDWSN is essential for many applications such as system security, scaling up of WSNs, and many more [15]. SDWSN is engaged with the challenges that are originated from SDN as well as WSN [16]. In this particular section, Table-I provides the allied work done of the recent 5 years (2014-2019) in the field of SDN and WSN together to form an emerging network architecture: SDWSN.

Revised Manuscript Received on October 10, 2019

\* Correspondence Author

**Shanu Bhardwaj\***, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. Email: shanu.bhardwaj@chitkara.edu.in

**S.N. Panda**, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.

**Chih-Yung Chang**, Department of Computer Science and Information Engineering, Tamkang University, Taiwan.

**Table- I: Work done in SDN and WSN**

Year	Paper	Objective
2019	Anadiotis et al. [17]	Introduced a paradigm SD-WISE which basically extends the capabilities of SDN to WSN to make the flow of the network more flexible.
2019	Luz et al. [18]	Monitor the performance of the SDWSN framework. It collects data of the transmitted packets, energy on each node and the information about the controller.
2019	Xu et al. [19]	Proposed a new mission-critical WSN based on SDN which resolves the issues of the traditional WSN like resource utilization, system compatibility, and latency requirements.
2019	Azizi et al. [20]	Proposed routing protocol for the energy efficiency for WSN by using SDN
2018	Thupae et al. [15]	Presented the challenges in the SDWSN for network management and security.
2018	Bhoi et al. [21]	Proposed a fault detection approach in the network based on SDN. The method used is found to be the best solution in WSN for the detection of the fault.
2018	Haque et al. [22]	Proposed an SDN based design for WSN for the maximum infliction of the network resources.
2018	Zhao et al. [23]	Proposed a routing algorithm of WSN based on SDN to track the routing of the information.
2018	Yan et al. [24]	Proposed an intrusion detection system with improved efficiency and the consumption of energy is also reduced.
2017	Ali et al. [25]	Presented the understanding of SDN and how the SDN overcomes the shortcomings in WSN.
2017	Wang et al. [26]	Proposed a routing algorithm based on SDN with multi-hop WSN.
2016	Bera et al. [27]	Proposed a system, Soft-WSN which focuses on the management issues for enhancing the flexibility of the WSN.
2016	Bizanis et al. [28]	Provided comprehensive study of SDN and NV in Wireless Sensor Network with real-time deployments.
2016	Wang et al. [29]	Proposed a sleep scheduling algorithm SDN-ECCKN based on SDN for the management of energy in the network.
2015	Jayashree et al. [30]	Proposed a substructure with the combination of SDN and WSN which provides an energy-saving architecture.
2015	Huang et al. [31]	The proposed architecture of SDWSN. The architecture model is efficient for reliability checking.
2015	Olivier et al. [32]	Proposed an architecture names ad Software-Defined Sensor Clustered Network basically used for the exchange of information from the controller to the other domains of SDN.
2014	Han et al. [33]	Proposed a solution based on WSN with the assistance of SDN in load balancing and changed the topology.

### III. SOFTWARE-DEFINED NETWORKING

SDN is a prominent system that hopes to change the curbs of the standard system framework by carrying the control functionalities together in a single zone [34]. SDN permits the isolation of its plane from a single device as a result, the control plane becomes the centralized controller and the switches become a forwarding device which forwards the data in an automated way [35].

SDN varies from conventional IP networks because the

forwarding of data packets is totally based on the flow despite packets [36]. Moreover, SDN proposed a centralized or consolidated control of the whole network by an application which permits the rapid management of the network [37]. Hence, the administrator of the network has programmable as well as centralized control of traffic in the network itself without involving an individual for the configurations of the hardware devices.

The technology, SDN can be used in many several scopes like networking, sensor network, security, IoT, data centers, and many more [38].

**A. Architecture of SDN**

SDN architecture shows how the SDN works in its different layers and how the SDN maintains the security, reliability and many other factors. Fig. 1 shows, the three layers of SDN which are as follows [39], [40]:

- **Data plane:** It is the same as one of the layer of OSI model (physical layer) which consists of network elements such as virtual devices and physical devices that contract with the network traffic. Data plane is well known as a forwarding layer/plane and is accountable for forwarding the frames of the packet from one hop to another hop.
- **Control layer:** It is the powerful plane in the SDN network which carries the data traffic and provides routing to traffic in the network. Several routing protocols such as RIP, BGP, OSPF, and EIGRP are managed by the control plane. Controllers in the SDN are used to extract the information from the devices and give it to the SDN applications. Management and the centralized configuration are the main functions of the control plane in SDN. The different controllers in SDN lie in the control plane are: Beacon, Ryu, NOX, Floodlight, POX and many more.
- **Application plane:** Different applications are used in the business networks that tells what to do to the network as per the business needs. Similarly, the Application Layer carry different applications according to the user needs. The API's are used by the controller to pass on the commands to the router to perform the particular task.

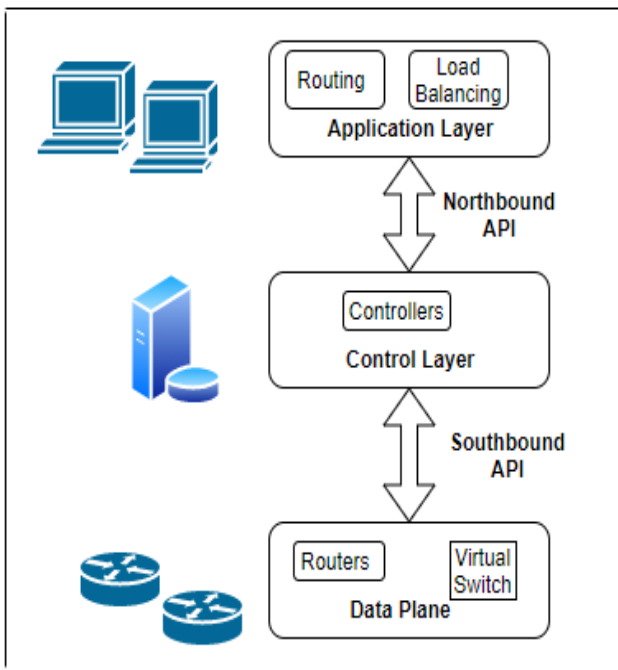


Fig. 1. The architecture of SDN.

**IV. WIRELESS SENSOR NETWORK**

WSN comprise of a deposit of autonomous sensors that are operate to detect or monitor the environmental and physical conditions like humidity, temperature and many more [12]. The different devices in the WSN are known as nodes. Nodes consist of a microcontroller, energy source and radio transceiver [41]. The characteristics of WSN are:

- **Scalability:** In the performance of the network, there is no interference of the deployment of the nodes [42].
- **Nodes Heterogeneity:** There is no need for the nodes in the network to contain the same characteristics [43].
- **Durability:** Nodes have the ability of resilience the environmental conditions [44].
- **Fault-tolerant:** Each node has the ability to subsist with the failure of the other nodes [45].

**A. Architecture of WSN**

The sensor field is the field that consists of different sensor nodes as shown in Fig. 2. These scattered nodes have the capability of collecting and routing the data by multi-hop architecture system to the user through application server. The application server communicates with the nodes that manage the tasks via Internet.

Depending upon the detecting tasks, on the application layer several sorts of software applications can be assembled and utilized. The maintenance of the flow of the data can be done with the help of the transport layer. The Internet/network layer which is accountable for the routing of data. The needs of robust, simple transferal and receiving are addressed by physical layer. The planes help in coordinating the sensing task for power consumption.

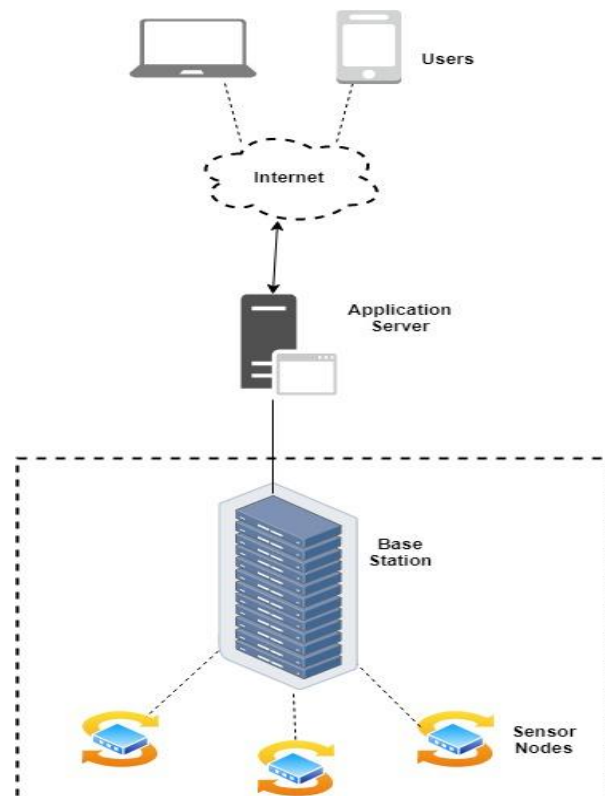


Fig. 2. The architecture of WSN.

## V. EMERGING TECHNOLOGY: SOFTWARE-DEFINED WIRELESS SENSOR NETWORK (SDWSN)

### A. Architecture of SDWSN

The architectures of SDN as well as SDWSN are analogous in terms of the management, seeing that, SDN is governed by the controllers and SDWSN is by the control sensor server. SDWSN is a three-layer SDN architecture in order to satisfy all the functionalities as depicted in Fig. 3. The data plane also known as physical layer which is commonly made up of different sensor nodes, base station and additionally consists of Software-Defined Ratio for controlling the media access. The control plane named as a networking layer is answerable for the transference of the data packets in the network. Lastly, Application layer is accountable for the management of the operative systems for controlling sensor nodes. The method of deployment of a new application is done via reprogramming the sensor node code within the network. Due to the high applicability of the WSN, SDWSN introduces a mechanism to alter the alignment of the network.

By this mean, the technological factor of the combination of both the technologies SDN as well as WSN known as SDWSN overcome a few of the limitations exists in the previous technologies.

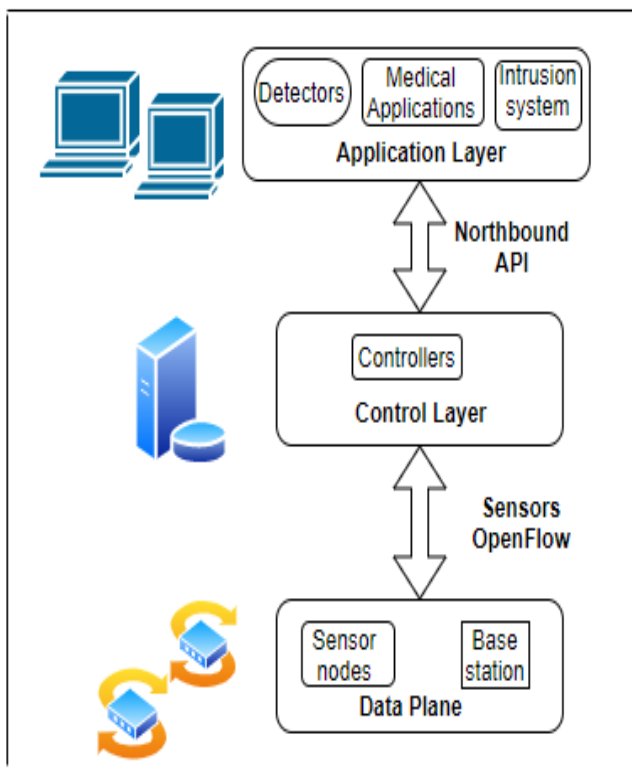


Fig. 3. The architecture of SDWSN.

### B. Challenges in SDWSN

- **Network Management:** In SD-WSN, management of the network is a tedious challenge and it can be studied in the

form of load balancing, traffic analysis, and fault tolerance. This inefficient challenge of network management needs to be marked to improve resource utilization in the network [46],[47]. Furthermore, the architecture of the network management should have the capability of differentiating the different types of traffic. One of the most essential tools in the management of the network is network monitoring tools [48]. In the traditional architecture networks shown in Table-II, the major focus is to reduce the response time as well as the energy usage in the network. It has been observed that the problem of management in net proceeds from the WSN. However, the management of WSN is an emerging research that has gained the attention of most of the research communities [49].

- **Energy Efficiency:** In SDWSN, the efficient usage of energy is a complex challenge and the efficiency of the energy can be maintained simply with the reduction of usage of energy by the devices [50]. However, due to the WSN's environmental security, the consumption of energy still remains an emerging issue in recent years. Some of the researchers suggested that the SDN is an encouraging technology for the management of sensor networks in form of energy efficiency [51]. Hence, by preventing the unnecessary loads while transmission can improve energy efficiency [52].



Table- II: SDWSN Challenges and Solutions.

Author	Challenge	Approach	Tool	Proposed Model
Costanzo et al. [53]	Resource allocation and management.	-	OpenFlow controllers	Proposed a scheme to manage the resources efficiently, energy-saving, and provides the flexibility to the routing path. The proposed scheme is categorized into three different layers: adaptive, virtualization layer, and the controller layer.
Galluccio et al. [54]	Reconfiguring	SDN-WISE	Sensor OpenFlow	Proposed SDNWISE, which is an extended version of the OpenFlow sensor. This is based on multiple local controllers and a single global controller. Here, the sensor participates in the local control only.
Gante et al. [50]	Wireless Sensor Network management	-	-	Proposed the solution for the management of WSN. With the help of the proposed solution, the Author inaugurated that the layer at which the controller is placed achieves much good performance in the management and also provides an energy-saving mechanism to the sensor nodes.
Zeng et al. [55]	Multitasking sharing of network resources	-	-	Proposed an architecture of SDN and WSN which supports multitasking sharing of the same network resources.
Akyildiz et al. [56]	Network Management for Traffic Engineering	SDN-TE	Wildcard	Proposed a query-based monitoring system based on the response as well as the request technique for the network management.
Shin et al. [57]	Security	FRESCO	OpenFlow controller	Proposed a solution for security that is implemented on the controller of OpenFlow.

- **Security:** SDN is the prominent networking approach that focus to untangle the management as well as the configuration of the network [58]. SDN eliminates the challenges that were faced by the traditional networks. Many solutions have developed just to address the security issues in the SD-WSN [59]. One of the proposed systems named “FRESCO” used to allow the security applications implemented on the controllers. However, interoperability with another network can enhance the efficiency of WSN’s [57]. WSN consists of a sizeable numeral of sensors node that is deployed over the network, in which the area where access is difficult and there is a great need for security such as for confidentiality, authentication, non-repudiation, and integrity.
- **Traffic Tolerance:** Traffic and fault tolerance are the issues that occur due to the tendency of WSN to the dynamic network such as the dropping of packets. To protect this network, the management should work with resistant to the dynamic network with the help of

SDN features such as the reconfiguration of the network. In the WSN, the failure in the way from the sensor node to communication can transpire at any time in the absence of pre warnings that can occur be a critical challenge comes into consideration. However, the challenges in network traffic management can be dealt by traffic tolerance [45].

### C. SDN based WSN solutions and features

Table-III shows SDN based WSN solutions as well as the key features. The first key feature, Resource issuance shows that this proposed solution has the capability of allocating the network resources. Next, Data aggregation indicates that the proposed solution aggregates the data to the network. The column OpenFlow stated that the current model is appropriate with the protocol named as OpenFlow. Finally, the management column indicates that the existing solutions manage the network efficiently.

Table-III: SDN based WSN solutions

Proposal	Resource issuance	Data Aggregation	OpenFlow	Management
SDWN [53]	✓	×	✓	✓
Multitasking SDN [60]	✓	×	×	✓
Sensor OpenFlow [61]	×	✓	✓	✓
Exploitation OpenFlow [62]	×	✓	✓	✓
SDN-WISE [54]	✓	✓	✓	✓
Smart WSN [50]	×	×	×	✓

## VI. CONCLUSION

SDN is the most essential network technology because of its management and revolutionary architecture. It also plays a vital role in security, scalability, reliability, and performance. SDN removed the challenges that were in the traditional networks and managed the changes in the network. However, SDN provides a centralized solution to retrieve the good performance.

WSN is the technology that is developed to execute specific applications. The major applications of WSN are industrial monitoring, health monitoring, and environmental monitoring. WSN provides mobility, versatility and many other factors to deploy anywhere. In WSN, security plays a imperative role in sending the data traffic to the whole network in a much-secured and automatic way.

With the union of SDN and WSN, an emerging paradigm has proposed, named as SDWSN. It is implemented to furnish the management of the sensor network. The birthing of SDWSN is essential in several applications such as scaling up of WSN and system security.

The finding of the paper is that SDWSN requires the utmost attention in the improvement of the energy consumption and management. Therefore, the paper presents some of the challenges inherited from the SDN and WSN to form the in SDWSN. The objective of the paper is to comprehend the challenges of SDWSN. Hence, these challenges still remain the issues and needs most of the attention of the researchers.

Thus, more and more techniques and tools can be designed and implemented in SDWSN to make the sensor network more secure, reliable, efficient, applicable and scalable. Taking into account that there is a great need to provide efficient solutions to these challenges in future.

## REFERENCES

1. D. L. Tennenhouse; J. M. Smith; W. D. Sincoskie; D. J. Wetherall; and G. J. Minden: A survey of active network research, *IEEE Commun. Mag.*, pp. 80–86, 1997, vol. 35(1).
2. K. Sood; S. Yu; and Y. Xiang: Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review, *IEEE*

3. S. Bera; S. Misra; and A. V Vasilakos: Software-defined networking for internet of things: A survey, *IEEE Internet Things J.*, pp. 1994–2008, 2017, vol. 4, no. 6.
4. Z. Qin; G. Denker; C. Giannelli; P. Bellavista; and N. Venkatasubramanian: A software defined networking architecture for the internet-of-things, in *2014 IEEE network operations and management symposium (NOMS)*, 2014, pp. 1–9.
5. B. Schwartz; A. W. Jackson; W. T. Strayer; W. Zhou; R. Rockwell; and C. Partridge: Smart packets for active networks, in *2nd Conf. on Open Architectures and Network Programming (OPENARCH'99)*, 1999.
6. B. Schwartz; A. W. Jackson; W. T. Strayer; W. Zhou; R. D. Rockwell; and C. Partridge: Smart packets: applying active networks to network management, *ACM Trans. Comput. Syst.*, pp. 67–88, 2000, vol. 18, no. 1.
7. M. Paliwal; D. Shrimankar; and O. Tembhurne: Controllers in SDN: A review report, *IEEE Access*, pp. 36256–36270, 2018, vol. 6.
8. L. Zhu; M. M. Karim; K. Sharif; F. Li; X. Du; and M. Guizani: SDN Controllers: Benchmarking & Performance Evaluation, *arXiv Prepr. arXiv1902.04491*, 2019.
9. I. F. Akyildiz; W. Su; Y. Sankarasubramaniam; and E. Cayirci: Wireless sensor networks: a survey, *Comput. networks*, pp. 393–422, 2002, vol. 38, no. 4.
10. J. Yick; B. Mukherjee; and D. Ghosal, Wireless sensor network survey, *Comput. networks*, pp. 2292–2330, 2008, vol. 52, no. 12.
11. N. Ntuli; and A. Abu-Mahfouz: A simple security architecture for smart water management system, *Procedia Comput. Sci.*, 2016, pp. 1164–1169, vol. 83.
12. M. M. Zanjireh; and H. Larijani: A survey on centralised and distributed clustering routing algorithms for WSNs, in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–6.
13. M. Castillo-Effer; D. H. Quintela; W. Moreno; R. Jordan; and W. Westhoff: Wireless sensor networks for flash-flood alerting, in *Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits and Systems, 2004*, pp. 142–146, vol. 1.
14. G. Werner-Allen *et al.*: Deploying a wireless sensor network on an active volcano, *IEEE Internet Comput.*, pp. 18–25, 2006, vol. 10, no. 2.
15. R. Thupae; B. Isong; N. Gasela; and A. M. Abu-Mahfouz: Software Defined Wireless Sensor Networks Mangement and Security Challenges: A Review, in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 4736–4741.
16. H. I. Kobo; A. M. Abu-Mahfouz; and G. P. Hancke: Fragmentation-Based Distributed Control System for Software-Defined Wireless Sensor Networks, *IEEE Trans. Ind. Informatics*, pp. 901–910, 2018, vol. 15, no. 2.
17. A.-C. Anadiotis; L. Galluccio; S. Milardo; G. Morabito; and S. Palazzo: SD-WISE: a software-defined wireless sensor network, *Comput. Networks*, pp. 84–95, 2019, vol. 159.

18. T. C. Luz; G. A. Nunez; C. B. Margi; and F. L. Verdi: In-network performance measurements for Software Defined Wireless Sensor Networks, in *2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC)*, 2019, pp. 206–211.
19. F. Xu; H. Ye; F. Yang; and C. Zhao: Software defined mission-critical wireless sensor network: Architecture and edge offloading strategy, *IEEE Access*, pp. 10383–10391, 2019, vol. 7.
20. M. S. AZIZI; and M. L. HASNAOUI: Software Defined Networking for Energy Efficient Wireless Sensor Network, in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019, pp. 1–7.
21. S. K. Bhoi; M. S. Obaidat; D. Puthal; M. Singh; and K.-F. Hsiao; Software Defined Network Based Fault Detection in Industrial Wireless Sensor Networks, in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.
22. I. Haque; M. Nurujjaman; J. Harms; and N. Abu-Ghazaleh; SDSense: An Agile and Flexible SDN-Based Framework for Wireless Sensor Networks, *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1866–1876, 2018.
23. Z.-N. Zhao; J. Wang; and H.-W. Guo, “A hierarchical adaptive routing algorithm of wireless sensor network based on software-defined network,” *Int. J. Distrib. Sens. Networks*, vol. 14, no. 8, p. 1550147718794617, 2018.
24. N. Yan and P. Zhang, “Software defined network intrusion detection in wireless sensor network,” in *MATEC Web of Conferences*, 2018, vol. 232, p. 4062.
25. N. F. Ali, A. M. Said, K. Nisar, and I. A. Aziz, “A survey on software defined network approaches for achieving energy efficiency in wireless sensor network,” in *2017 IEEE Conference on Wireless Sensors (ICWiSe)*, 2017, pp. 1–6.
26. J. Wang *et al.*, Software defined network routing in wireless sensor network, in *Cloud Computing, Privacy in New Computing Environments*, Springer, 2016, pp. 3–11.
27. S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, “Soft-WSN: Software-defined WSN management system for IoT applications,” *IEEE Syst. J.*, 2016, vol. 12, no. 3, pp. 2074–2081.
28. N. Bizanis and F. A. Kuipers, “SDN and virtualization solutions for the Internet of Things: A survey,” *IEEE Access*, 2016, vol. 4, pp. 5591–5606.
29. Y. Wang, H. Chen, X. Wu, and L. Shu, “An energy-efficient SDN based sleep scheduling algorithm for WSNs,” *J. Netw. Comput. Appl.*, 2016, vol. 59, pp. 39–45.
30. P. Jayashree and F. I. Princy, “Leveraging SDN to conserve energy in WSN-An analysis,” in *2015 3rd International conference on signal processing, communication and networking (ICSCN)*, 2015, pp. 1–6.
31. Y. Lu *et al.*, “A study on the reliability of software defined wireless sensor network,” in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015, pp. 129–134.
32. F. Olivier, and N. Florent, SDN based architecture for clustered WSN, *9th International Conference on Innovative Mobile and Internet in Ubiquitous Computing*, 2015, pp. 342–347.
33. Z. Han and W. Ren, A novel wireless sensor networks structure based on the SDN,” *Int. J. Distrib. Sens. Networks*, 2014, vol. 10, no. 3, p. 874047.
34. A. L. Caraguay; A. L. I. Barona Lopez, and L. Villalba; SDN: Evolution and opportunities in the development IoT applications, *Int. J. Distrib. Sens. Networks*, 2014, vol. 10, no. 5, p. 735142.
35. O. Salman, I. H. Elhadj, A. Kayssi, and A. Chehab, “SDN controllers: A comparative study,” in *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, 2016, pp. 1–6.
36. D. Kreutz, F. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *arXiv Prepr. arXiv1406.0440*, 2014.
37. N. A. Jagadeesan and B. Krishnamachari, “Software-Defined Networking Paradigms in Wireless Networks: A Survey,” *ACM Comput. Surv.*, 2014, vol. 47, no. 2, pp. 21–27.
38. P. Sanchez, R. Lopez, and A. Skarmeta, “Pاناتiki: A network access control implementation based on pana for iot devices,” *Sensors*, 2013, vol. 13, no. 11, pp. 14888–14917.
39. S. Sezer *et al.*, “Are we ready for SDN? Implementation challenges for software-defined networks,” *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, 2013.
40. R. Braga, E. de Souza Mota, and A. Passito, “Lightweight DDoS flooding attack detection using NOX/OpenFlow,” in *LCN*, 2010, vol. 10, pp. 408–415.
41. S. Bhardwaj and S. N. Panda, “A Study on Noninvasive Body Wearable Sensors,” in *Intelligent Communication, Control and Devices*, Springer, 2020, pp. 345–351.
42. C. Vandana, “Security improvement in iot based on software defined networking (sdn),” *Int. J. Sci. Eng. Technol. Res.*, vol. 5, no. 1, pp. 2327–4662, 2016.
43. H.-S. Chai, J.-Y. Choi, and J. Jeong, “An enhanced secure mobility management scheme for building iot applications,” *Procedia Comput. Sci.*, vol. 56, pp. 586–591, 2015.
44. E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, “On the security and privacy of internet of things architectures and systems,” in *2015 International Workshop on Secure Internet of Things (SIoT)*, 2015, pp. 49–57.
45. C. Yu, Y. Cui, L. Zhang, and S. Yang, “Zigbee wireless sensor network in environmental monitoring applications,” in *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, pp. 1–5.
46. J. Gubbi, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Comput. Syst.*, pp. 1645–1660, 2013, vol. 29, no. 7.
47. M. Amadeo *et al.*, “Information-centric networking for the internet of things: challenges and opportunities,” *IEEE Netw.*, pp. 92–100, 2016, vol. 30, no. 2.
48. S. Bera, S. Misra, and M. S. Obaidat, “Mobility-aware flow-table implementation in software-defined IoT,” in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–6.
49. H. Kim and N. Feamster, “Improving network management with software defined networking,” *IEEE Commun. Mag.*, pp. 114–119, 2013, vol. 51, no. 2.
50. A. De Gante, M. Aslan, and A. Matrawy, “Smart wireless sensor network management based on software-defined networking,” in *2014 27th Biennial Symposium on Communications (QBSC)*, 2014, pp. 71–75.
51. Z. Shu *et al.*, “Traffic engineering in software-defined networking: Measurement and management,” *IEEE access*, 2016, vol. 4, pp. 3246–3256.
52. K. M. Modieginyane, R. Malekian, and B. B. Letswamotse, “Flexible network management and application service adaptability in software defined wireless sensor networks,” *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 4, pp. 1621–1630, 2019.
53. S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, “Software defined wireless networks (sdwn): Unbridling sdn,” in *European workshop on software defined networking*, 2012, pp. 1–6.
54. L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, “SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for Wireless Sensor networks,” in *2015 IEEE Conference on Computer Communications (INFOCOM)*, 2015, pp. 513–521.
55. D. Zeng, P. Li, S. Guo, T. Miyazaki, J. Hu, and Y. Xiang, “Energy minimization in multi-task software-defined sensor networks,” *IEEE Trans. Comput.*, vol. 64, no. 11, pp. 3128–3139, 2015.
56. I. F. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, “Research challenges for traffic engineering in software defined networks,” *IEEE Netw.*, vol. 30, no. 3, pp. 52–58, 2016.
57. S. W. Shin, P. Porras, V. Yegneswara, M. Fong, G. Gu, and M. Tyson, “Fresco: Modular composable security services for software-defined networks,” in *20th Annual Network & Distributed System Security Symposium*, 2013.
58. S. W. Pritchard, G. P. Hancke, and A. M. Abu-Mahfouz, Security in software-defined wireless sensor networks: Threats, challenges and potential solutions, in *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*, 2017, pp. 168–173.
59. D. Kreutz, and P. Verissimo, Towards dependable software-defined networks, in *Proceedings of the ACM workshop on topics in software defined networking*, 2013, pp. 55–60.
60. D. Zeng, T. Miyazaki, S. Guo, T. Tsukahara, J. Kitamichi, and T. Hayashi, “Evolution of software-defined sensor networks,” in *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, 2013, pp. 410–413.
61. T. Luo, H.-P. Tan, and T. Q. S. Quek, “Sensor OpenFlow: Enabling software-defined wireless sensor networks,” *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1896–1899, 2012.
62. A. Mahmud and R. Rahmani, “Exploitation of OpenFlow in wireless sensor networks,” in *Proceedings of 2011 International Conference on Computer Science and Network Technology*, 2011, vol. 1, pp. 594–600.

## AUTHORS PROFILE



**Shanu Bhardwaj** is currently pursuing M.tech (Computer Science and Engineering) from Chitkara University, Punjab, India. She has completed her B. Tech (Computer Science and Engineering) from Kurukshetra University, Kurukshetra (India). Her research areas are Software-Defined Networking, Internet of Things (IoT), Wireless sensor network (WSN) and

Network security. She has completed her internship on "Application of Big Data in Construction Law" from Tamkang University, Taiwan.



**Dr. S.N. Panda** has completed his Ph.D., M.Sc in the field of Computer science from Kurukshetra University, India, Bachelor of Science with honors from Sambalpur University, India. PGDEDP from NIEL-IT, Chandigarh and PGDCA from Kurukshetra University. He is currently working as Director (Research) in Chitkara University, Punjab, India. He is having 25+ years of research experience of He has guided 11 PhD scholar and

13 M.Phil students. His major research areas includes Machine Vision, Communication networking and Protocol, Internet of Things, Big Data, network security, e-governance, e-business. Technology Trends, Security etc.



**Chih-Yung Chang** completed his Ph.D. in 1955 (Computer Science and Information Engineering) from the National Central University, Taiwan. He is currently working as a Professor in the Department of Computer Science and Information Engineering, Tamkang University, Taiwan. His research area includes, wireless sensor networks, Internet of things, Artificial Intelligence, and deep learning. He is also an Associate Guest Editor for several SCI-indexed journals, including the

International Journal of Ad Hoc and Ubiquitous Computing (IAHUC) from 2011 to 2014, the International Journal of Distributed Sensor Networks (IJDSN) from 2012 to 2014, IET Communications in 2011, Telecommunication Systems (TS) in 2010, the Journal of Information Science and Engineering (JISE) in 2008, and the Journal of Internet Technology (JIT) from 2004 to 2008.