Science Arena Publications
Specialty Journal of Electronic and Computer Sciences
ISSN: 2412-7485
Available online at www.sciarena.com
2019, Vol, 5 (3): 66-74

Software Defined Wireless Sensor Networks: A Survey

Sahar Abdipoor

Department of computer, computer Engineering, University of ahvaz, Barkhat University, Ahvaz, Iran.

Abstract: *Wireless Sensor Networks (WSNs) are commonly used information technologies of modern networking and computing platforms.Wireless Sensor Networks (WSN) consist of low power devices that are distributed in geographically isolated areas. Sensors are arranged in clusters. Each cluster defines a vital node which is known as a cluster head (CH). Each CH collects the sensed data from its sensor nodes to be transmitted to a base station (BS). Sensors have deployed with batteries that cannot be replaced. The energy consumption is an important concern for WSN. Today's network computing applications are faced with a high demand of powerful network functionalities. Functional network reach is cen- tral to customer satisfaction such as in mobile networks and cloud computing environ- ments. However, efficient management of WSNs remains a challenge, due to problems sup- plemental to them. Recent technology shift proposes Software Defined Networking (SDN) for improving computing networks. This review paper highlights application challenges faced by WSNs for monitored environments and those faced by the proposed approaches, as well as opportunities that can be realized on applications of WSNs using SDN. We also highlight Implementation considerations by focusing on critical aspects that should not be disregarded when attempting to improve network functionalities. We then propose a strat- egy for Software Defined Wireless Sensor Network (SDWSN) as an effort f or application improvement in monitored environments.*

Keywords: *Wireless sensor networks, Software defined networking, Internet of things, Software defined wireless sensor networks.*

INTRODUCTION

WSNs are sensor network technologies which are widely deployed on environmental monitoring, atmospheric monitor- ing, process monitoring, material sensing, security applications, etc. These networks operate on collective networking and computing of individual sensors based on their physical sensing properties and processing capabilities. Sensors nodes, coop- eratively communicate and relay aggregated data to the main network control system for further processing and acting. In this regard, these sensors, must have an ability to conform to the collective networking functionalities as governed by their respective network policies. In WSNs, sensor nodes can be randomly deployed, in essence allowing opportunities for applications even in inaccessible areas. This feature about sensor networks, allows the possibility of deploying a large number of sensors over intuited areas for as long as communications can be established and sustained among these sensor nodes. A WSN consists of, but not limited to; a WSN server, routers, switches, sensor nodes, etc. depending on the design setup as required for its purpose. In this paper, we consider challenges experience in WSN applications. We provide brief introductions to both SDN and SDWSN and also highlight their technological prospects in WSN applications. This paper further considers challenges that are

WSN case studies

- **General perspective for designing WSN application systems**

To design deployable and functional WSN systems, several factors and elements needs to be made in terms of case studies. As the same as with other systemic technologies, the development of each WSN application system is led by a requirement or need for that system. These requirements are at times influenced by technology markets or ongoing research approaches and developments. Following this phase, case studies are conducted to best understand the requirements, factors, elements, constraints, strategies and the feasibilities for implementing these technologies. For WSNs, these studies include but not limited to; understanding the size of the network to be designed, hardware and software requirements for the network design, the cost to implement the network as well as the resources to sustain and maintain that network. Other important case studies include; human related factors and the area wherein the network will be deployed

- **Detailed factors for developing WSN application systems**

Due to the technological market and research developments as described above, application systems need to solve a certain problem. This leads to a more detailed understanding and listing of technical requirements in terms of hardware and software needed to build these systems. These technical aspects include;1) the type of sensor hardware to be used, 2) operational characteristics of these sensors, 3) operational platform to deploy these application systems and 4) choice of routing protocols and considerations for operational standards, for both the network infrastructure, sensors, etc. Other technicalities to be considered include; mechanisms for power resources for these systems, data mining aspects, level of radio frequency operation and identification and scalability options for the network design.

WSNs routing protocols and network topologies

- **Routing protocols**

To improve WSN system operations and applications, several access and routing protocols have been developed and applied which include but not limited to the following: _ *Medium Access Control* (MAC) protocol – whose main strategy is to reduce energy consumption, since sensor nodes in a WSN systems are battery powered thereby resulting in a limited network lifetime. _ *Low Energy Adaptive Clustering Hierarchy* (LEACH) protocol – which is the fundamental protocol to propose some level of data fusion as well as a focus to implement a strategy for low power utilisation in hierarchical WSNs. _ *Ad hoc On-Demand Vector* (AODV) routing protocol – its main objective is to reduce packets flooding which causes over-head within the network. One critical functionality of this protocol is to utilize routing tables to store routing informa-tion. _ *Sensor Protocols for Information via Negotiation* (SPIN) – These types of protocols are based on sensor nodes negotiations for allowing data transmission and resource adaptation mechanisms for energy saving. _ *Geographic and Energy Aware Routing* (GEAR) protocol – It is based on the energy and location of sensor nodes which are on their transmission paths towards their targeted regions. Its implementation facilitates the trade-off between energy and distance. Table 1 discusses the advantages and disadvantages of the protocols discussed above.

- **Network topologies**

Commonly known WSN topologies are described below. Other forms of sensor network topologies are designed as a combination or extension of these network topologies due to the design requirements decided for different deployments.

Please cite this article as: K.M. Modieginyane et al., Software defined wireless sensor networks application opportunities for efficient network management: A survey, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.02.026

Table 1 : Advantages and disadvantages of WSN Protocals.

Protocal	Advantages	Disadvantage
MACl		Energy wastage
LEATCH	Increases Network Life time Energy Saving due to aggregation by CHs.	Dynamic clustering brings extra overhed Cannot ensure real load balancing in the case of sensor nods with different amounts of initial energy Nodes use single-hop communication
AODV	Connection setup delay is less Routers are established on demand	Intermediate nodes can lead to inconsistent routes Multiple Route Request Packet in response to a single route Request Packet can lead to heavy control overhead.
SPIN	Topological changes are localised	Not certain the data will reach the destination or not. If the nodes that are interested in the data are far away from the source node And the nodes between source and destination are not interested in that data. Such data will not be delivered to the destination at all. Idle nodes consume energy.
GEAR	Increases Network Lifetime Help in balancing energy consumption	

Table 2: Advantages and disadvantages of WSN topologies

Topology	Advantages	Disadvantages
Star	Node failure does not affect other nodes Low Power consumption	If central node fails, the whole network wont be able to work low transmission range
Tree	low power consumption High transmission range	Topology is very complexy Not resilient to node failure Uneven power consumption across nodes
Mesh	High fault tolerance	High power consumption Increased latency Redundant paths
Hybride	low power consumption Fault tolerant Reliable communication	

I *Star topology* : –In this type of a network structure, sensor nodes transmit data only through a central device. Considered for small networks. A failure in any sensor node except the central device, does not affect the network or other sensor nodes. Not expensive to implement this architecture, as nodes share one central device

II *Tree topology* : - Efficient for optimizing the power consumption or to extend the communication range of the network. Some level of scalability can be achieved in this type of a network. This architecture can be easily managed or maintained since the network is divided into branches or segments. If the root node fails, the lower structure also fails. This network design is not expensive to implement.

III *Mesh topology* : - All the sensor nodes within the same radio or communication range are connected. To reach a far destination device, data is transmitted through neighbouring nodes. Very fault tolerant since there are a lot of path options for other sensor nodes to successfully transmit data should one node fail. However, it is expensive to implement this type of a network.

IV *Heterogeneous topology* : - This results as a form of combination of two or more of the above topologies. This type of a network implementation is somehow, reliable, scalable, flexible and effective in its operation. However, it is expensive to implement, since it is a combination of two or more network topologies of different capabilities. Table 2 discusses the advantages and disadvantages of the topologies discussed above.

WSN challenges and deployment considerations

Even though WSNs are popular due to their simplicity of deployment and cost effectiveness, managing them is a difficult task pointing to their resource constrained nature. However, applications of WSNs have continued to grow regardless of the challenges experienced in their use. Basically, WSNs are envisioned to be deployed on large scale, as millions of wireless sensor nodes will be working cooperatively to transmit critical data and as well being connected to the internet as an effort for the realization of internet of things (IoT). WSN technologies have been successfully developed and implemented in a wide range of applications as discussed be- fore. These technologies are now commercialized according to their range and specificity of application.

Systems such as those used in health, military and environmental monitoring are some of the most commercialized tech- nologies around the area WSNs. These technologies play a pivotal role in everyday living as some of them are mission critical systems. The wide adoption of WSN technologies is since these systems are affordable and not difficult to implement. How- ever, the cost of implementing such technologies depends on their range (in terms of size and purpose) of operation. Due to factors, such as their affordability, ease to expand and not conforming to a particular network topology, WSN technologies could be adopted and optimized as the fundamental structure for the IoT network paradigm. Commonly reported challenges include; sensor node energy limitations, low memory and processing capacity, low chan- nel bandwidth and being application specific. A lot of work has been done particularly on energy limitations as an effort to improve the node energy utilization on WSNs. In addition to that, other methods of energy harvesting have been proposed as a means to leverage this limitation on sensor nodes. However, the energy issue is still a serious challenge in WSNs since it affects the lifetime of a WSN directly. Other challenges include high latency in communication, traffic congestion and processing delays on intermediate nodes due to the packet-based routing nature of WSNs. Based on the proposed strategy, another controller functionality could be to write container rules or applications which will operate on certain network devices such as routers and programmable sink nodes. This functionality could be used to apply software focused strategies which will be responsible for load balancing, ensuring resourceful bandwidth utilization as well as perform quick search operations for data transmission to complement efficient processing, thereby reducing high delays. Since WSNs are energy and processing constrained, important considerations must be made before the deployment phase of the network. These considerations includes, but not limited to; understanding phenomena/event requirements and the de- ployment environment (as this will assist in deciding on relevant equipment and their capability, and also whether there are no radio frequency disturbances within the area, sensor network connectivity, the ability of the network to self-configure in adverse or intrusion situation, choice of wireless protocol depending on the sensor type to be used as protocols/standards differ in power usability, throughput and communication range. We therefore put emphasis towards these considera- tions, so that if necessary; any software or resource oriented limitation be accounted for during the network planning phase.

SDN and its implementation challenges

- **Case studies for designing SDN**

The concept of implementing SDN strategies to modern computer networks is imagined as a possible solution for com- mon challenges experienced on them. However, due to the novelty of this networking paradigm, it remains unclear as to how this strategy can be fully applied to the effectiveness of today's networking technologies. In this paper, we carry out case studies for designing SDN strategies for most network environments. To start with, we discuss components that makes up a functional network, since these are critical when designing any network. A network is a platform of inter-linked, con- nected or interfaced hardware and software developed and operated by either human or machine capacity. It is therefore, an involving task to implement a functional network that uses new computing strategies such as SDN in production networks. Case studies carried out in this paper, reveals some systematic and situational challenges that needs to be considered when designing SDN technologies. These includes; 1) The type and cost of infrastructure to host and support this new technology, 2) The capacity or skilled personnel required to operate or maintain the network, 3) Platforms and software needed to command the network, 4) Security levels and features which will be required for this technology. Other critical aspects that could be considered include; a) The risk of shifting to a new technology as opposed to optimizing the working old technology, b) The task of developing new procedures, protocols and applications which will support the new technology. It is therefore, important to understand and properly implement the functionalities of each component needed to support any new technology. Please cite this article as: K.M. Modieginyane et al., Software defined wireless sensor networks application

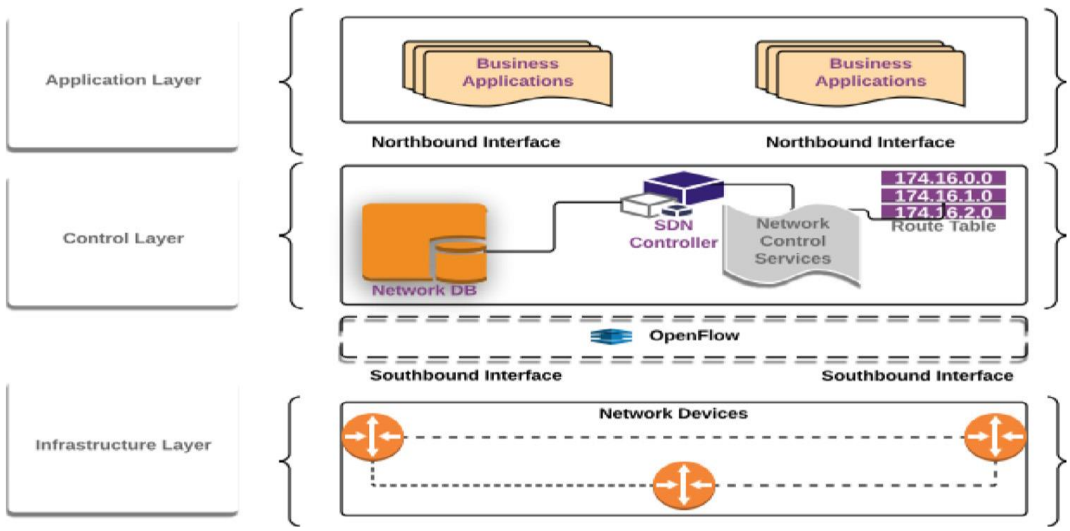

Figure 1. An overview of SDN architecture.

- **SDN architecture**

SDN is a framework that decouples the control plane and the data plane to allow network administrators to automatically and dynamically manage and control numerous network devices, services, topology, traffic paths, Quality of Service (QoS) and packet handling policies using high level programming languages and Application Programming Interfaces (APIs) of their choice (Jain, 2013). We also describe an SDN approach using OpenFlow as shown in Fig. 1 above. OpenFlow by Open Networking Foundation (ONF); is a standard communications interface defined between the control and forwarding layers of an SDN architecture, which allows direct access to and manipulation of the forwarding plane of network devices such as routers and switches, both physical and virtual (hypervisor-based) (McKeown et al., 2008). Even though SDN applications promise to improve the overall networking experience by shifting complex processing functionalities from the network equipment to the controller, SDN itself has its own implementation challenges most espe- cially on existing networks such as; infrastructural support for smooth transitions to SDN environments, flexible hardware for SDN deployment or applications, etc. However, as part of the proposed approach, this work intends to solve this prob- lem by implementing controller functionalities that will be able to store current processing states and concurrently perform some automation on the base Operating System (OS) to support critical network devices for abstracted operations. This could also allow opportunities to implement virtual network components which will act as actual devices in performing other network state applications. Other concerns and challenges are that; a steady development is still needed to apply SDN concepts at network infrastructure level, since there is currently no general accord yet on how the programmable logic can be achieved, since there is currently no global standardization for SDN.

- **SDN challenges and opportunities in WSNs**

Today's network computing applications are faced with a high demand of powerful network functionalities and per- formance. This high demand is mainly motivated by advancements in the area of computing spanning provider networks, data centers, cloud computing environments, etc. However, resourceful management of WSNs is a serious challenge, due to problems supplemental to them. Conversely, advancements and improvements in the manufacturing of computing or networking devices has awarded researchers and developers opportunities to experiment on these devices as an effort to enhance network computing capabilities and experience. Upon these concerns, recent network technology shift proposes SDN as a means to improve computing networks. An improvement position is that, since resource management and process control are so difficult in WSNs due to their sensor properties and structural complexity, SDN aims at bringing convenient control mechanisms to WSNs. Current stud- ies indicate that this capability will allow the controlling unit (the controller) to easily manage network resources as well as preparing a platform for other networking applications. One of the main objectives of SDN strategy is to ease up the process of network management. Primarily, SDN transforms a network administration problem into a simplified network programmable one. The suggestion is that by applying SDN, the complexity of sensor networks management can be simpli- fied. With the flexibility gained by the introduction of SDN to sensor networks new protocols can be employed very easily without the need to reprogram or reconfigure any sensor node. Distinctively, one of the core strategies of SDN in computing networks is to make an effort of visualizing the network architecture more clearly and comprehensive, as this could; 1) Make it easier for network operators to study and understand the network, 2) Allow operators to quickly come up with measures that are most relevant for specific network problems, 3) Encourage innovation in computing networks to prepare for or meet future demands, 4) Allow easy access of network resources so as to manipulate them as necessary and 5) Improve the way computing networks are observed or visualized and thus permitting network operators to easily manage and maintain adjacent network resources.

- **SDN versus traditional network (Non-SDN network)**

Some arguments still exist in terms of management and performance of SDN based networks and traditional network. These arguments are mainly looked at as comparisons between these two network technologies as an effort to highlight which technology brings benefits. These arguments are also further interpreted to the act of making decisions as to which technology could be used and for what intent that technology could be used. Table 3 gives these arguments in terms of comparisons.

Table 3: Comparison between an SDN network and a traditional network.

Potential	SDN	Traditional(Non-SDN)network
Operate Features	separation of the control and forwarding planes. Easily Controlled and deloyed.	Hard-structured and logically coupled operation.very Coplex control.
Implementation	Fast and easily implemented. Adapt to the need of application Environments.	Time involving to implement. operate on dedicated Environments.
Management	Easily management using APIs. Can be easing modified depending On the network demand.	Difficult to manages as network devices are solely properietary And hard to access.
Stability	Currently unstable with few technological supports.	Stable with great network supports.

Security in SDN

Each and every systematic platform, structure or environment must entail some level of security. In general security is an integral part of every computing systems. Most importantly, security in these computing systems or devices must be considered and be accounted for during the planning phase of such systems. In addition to securing these systems, each system must be incorporated with intelligent security measures that the system should undertake at times when the system is compromised. We then emphasized that, as improvements in computing networks are such highly anticipated; security must be well thought of. Security in SDNs is still a major concern. In this regard, the following questions arises:

- How will security be implemented in SDN infrastructure?
- If implemented in a central point only (e.g. central controller), what will happen in the event where the controller is intruded?

-Please cite this article as: K.M. Modieginyane et al., Software defined wireless sensor networks application opportunities for efficient network management:
A survey, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.02.026

Software defined wireless sensor networks (SDWSN)

This section covers the SDWSN case studies, general overview of SDWSN, existing work, challenges and technological considerations regarding the adoption of the SDWSN concept.

- **Case studies for designing SDWSN application systems**

Several technologies of WSN systems have been used for a wide range of applications due to their simplicity of imple- mentation and cost effectiveness. Even though this has been the case, the high demand for extensively powerful systems of WSNs has rendered older technology systems and strategies to be less effective. This has therefore resulted in exploring other approaches for either optimizing current WSN application systems or developing new technologies. After conducting some literature survey around WSNs to improve their applications as well as testing some operations of WSNs applications through simulations, this work proposes a SDWSN system strategy as illustrated in Fig. 2 as a possible solution for challenges experienced in WSN application systems. Case studies together with some simulation results have revealed some limitations in these types of systems even though they are operational to some extent. Technical limitations learned from the conducted studies include; a) Lack of innovation in current WSN strategies to cater for compute intensive applications that require highly responsive systems, b) Inability to support concurrent processes for different application needs, c) Lack of global access to operate different network devices, d) Highly involved tasks of detecting and troubleshooting faulty network points and e) Difficulty in deploying new efficient protocols in an effort to optimize the overall network performance.

- **Strategies for developing SDWSN systems: solving WSN challenges**

The main drive to implement SDWSN is motivated by the SDN paradigm strategy to implement flexible and simple to manage computer networks. In addition to this, SDWSN strategy aims to implement networking technologies that allows the central view of the whole network. This paradigm change also introduces some level of programmability in production or application networks as a means to empower system administrators as well as network engineers to easily manage and optimize these networks. As a direction to implement SDWSN systems that can solve WSN application systems challenges listed in 7.1, several key elements have been identified as possible solutions to decline these fundamental limitations such as: a) The need to develop software-oriented protocols for WSN systems which will be mandated to cater for different application processes on the fly, b) The process of developing software injection techniques to support programming abstractions for sensor networks - As this will influence the manufacturing platform for open programmable sensor, c) The course of develop highly encryptedsoftware oriented algorithms to secure the control and data plane, d) To develop software strategies which will be respon- sible for data manipulation and presentation and e) To develop controller application strategies for accessing and updating sensor properties to best suite different application needs and operation parameters.

- **Challenges and considerations**

One critical challenge in SDWSN is the efficient assignment of spectrum resources to the virtual network, which then contributes to the spectrum resource problem. However, dynamic programming and graph theory based spectrum sharing algorithm is proposed in (Yang et al., 2014), wherein a performance improvement in this regard was achieved. Once more, there is a concern as to say; since SDN propose to facilitate a control of the underlying network from a dedicated point, it is alleged that the whole network will collapse in case where the controller is disrupted or somehow fail. Also, with the current envision about Internet of Things through WSNs (Wang et al., 2016; Wannenburg, 2015), it must be considered as to whether a relevant infrastructure can be realized on SDWSN. Subsequent to uncertainties that surrounds the standard architecture as well as the effective adoption of SDN technolo- gies in production or application networks, some level of understanding is needed regarding its structural components and the fundamental benefits that SDN proposes to bring. Due to the distinctive architectural model of SDN, network customiza- tion (Cloete and Nair, 2016) and resource optimization in WSNs could be achieved using this approach, thereby improving the overall network performance. SDN is also aimed at providing network stability and flexibility in WSNs, through the enhancement of some of the critical network aspects such as; process scheduling, traffic routing, resource access, network abstraction and pro- grammability. Congruently, SDWSN aims at improving resource utilization and “open”network programmability in WSNs.

Future directions: technology and research opportunities

Looking at the radical improvements and changes in today’s network computing as well as reported achievements in this field, it is most certain that in the future more sophisticated but easy to use and manage technologies will be realized. Some level of attention needs to be drawn towards the SDN/OpenFlow northbound and southbound interfaces as these parts of the framework are of empirical means to the overall technological approach. We project that these interfaces still need to be further explored for efficient network understanding as well as resource optimization. In terms of future, we have identified the following research opportunities; 1) SDN controller virtualization for multi-controller sensor clusters, 2) Enhanced global network experience: Improvements on northbound interface communication, 3) Southbound interface optimization for efficient device access and controller communication and 4) SDN strategies for runtime and computationaloverhead in sensor clusters.

Conclusions

This paper looked at challenges experienced in WSNs as well as making critical analysis as to why careful considerations must be made before the deployment of WSNs especially for monitoring applications. Critical factors affecting applications of WSNs have also been discussed with advices that needs to be considered towards the network planning phase. We have also proposed a method of implementing simple state rules on the sink node as an effort to improve the SDWSN programmability as well as to offload the controller of such low-level compute tasks. As a technological position, information regarding current developments using SDN techniques have been provided. Based on the studies conducted in this survey, we envision the SDN approach in WSNs to be a promising direction, as this approach will extremely evolve these application systems.

References

1. Cloete NA, Nair L. Design of smart sensors for real-time water quality monitoring. IEEE Access 2016;4:3975–90.

2. Jain R. Introduction to software defined networking (SDN); 2013. available at: http://www.cse.wustl.edu/ ~jain/cse570-13/ .
3. McKeown N, Anderson T, Balakrishnan H, Parulkar GM, Peterson LL , Rexford J , etal. OpenFlow: enabling innovationincampus networks.Comput Commun Rev 2008;38(2):69–74
4. Wang Z, Ye N, Wang R, Li P. TMicroscope: Behavior perception based on the slightest RFID tag motion. Elektronika ir Elektrotechnika 2016;22(2):114–22.
5. Wannenburg J. Body sensor network for mobile health monitoring, a diagnosis and anticipating system. IEEE Sensors Journal 2015;15(12):6839–52.
6. Yang M, Li Y, Jin D, Su L, Zeng L. Opportunistic spectrum sharing in software defined wireless network. IEEE J Syst Eng Electron 2014;25(6):934–41.