ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Defining Wireless Sensor Networks in Software Approach

K Mythri Sridevi
Department of Computer Science and Engineering, JNTUK, Kakinada, Andhra Pradesh 533003, India.

Ravi Kiran K
Department of Computer Science and Engineering, JNTUK, Kakinada, Andhra Pradesh 533003, India.

B Hemanth Kumar
Department of Computer Science and Engineering, JNTUK, Kakinada, Andhra Pradesh 533003, India.

M Aruna
Department of Computer Science and Engineering, JNTUK, Kakinada, Andhra Pradesh 533003, India.

ABSTRACT:
Wireless sensor networks (WSNs) have well known limitations such as battery energy, computing power and bandwidth resources that sometimes limit their widespread use. Current researches are mainly concentrated to propose solutions for nodes energy optimization, network load balancing and the improvement of WSN robustness; however, the software defined network (SDN) paradigm uses the theory of forwarding phase separating from control, simplifying management and configuration of the network to improve network extension and flexibility. It could further optimize WSNs deployment and improve their transmission performance. In this paper, we firstly describe the general architecture and the main features of software defined networks; then, we analyze the current integrated SD-WSN scheme and summarize these results in detail.

Keywords: ***Software Defined Networking (SDN), Sensor Open- Flow, Wireless Sensor Networks (WSNs), OpenFlow.***

1. INTRODUCTION

Software-defined networking (SDN) is an emerging networking architecture that gives the opportunity to overcome the current limitations of the network infrastructure [1], [2]. It decouples the network's control plane and data plane. That means an intelligent controller configures forwarding elements with forwarding rules for data packets of different flows. The controller obtains sufficient information to fulfill that task so that distributed control protocols among forwarding elements are no longer needed. Furthermore, the controller may interact with applications to optimize the network.

Software-defined WSNs (SD-WSNs) have been recently proposed with the objective that WSNs can particularly profit from SDN. The operation of sensor nodes should be simplified to save energy and to manage the WSN through a powerful controller which has a view on the entire network rather by distributed control protocols. The controller is able to manage the network and applications while saving energy and to deliberately balance the residual energy of the network to maximize its lifetime. A significant difference to SDN in a datacenter is that the controller in a WSN communicates with distant sensor nodes over possibly multiple hops rather than over a dedicated control network.

In this survey, we give an introduction to SDN in wireline networks and to non-SDN WSNs. We describe the architecture of SD-WSNs, illustrate their operation, point out advances and research challenges. We also compare SDN-based and non SDN-based WSNs.

General Requirements for deploying SDN in WSNs are surveyed in [3], [4]. Ndiayeet al. [4] focused on how WSN management can be performed by SDN. Kobo et al.[3]concentrated on the architectural view of SDN in

Cite this article as: K Mythri Sridevi, Ravi Kiran K, B Hemanth Kumar & M Aruna, "Defining Wireless Sensor Networks in Software Approach", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 7 Issue 1, 2020, Page 1-13.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

WSNs. The authors of [5], [6] provided a survey on the application of SDN in wireless networks. However, none of these papers surveyed what can be controlled by SDN in WSNs and how applying SDN in WSNs is different from wire line networks.

2. WSNBASICS

In this section we briefly introduce the basic concepts of WSNs by giving a general overview on the network structure, use cases, standards, and research challenges.

A. Network Structure

In a WSN, each sensor node has a sensing region that can sense the events and objects within that range. Additionally, each node can communicate over a wireless interface with other nodes that are in the communication range of this node. Fig. 1 shows a collection of sensors that are scattered over a network area to monitor events, e.g., the event E in the figure. The information gathered from this event is transferred to a base station (BS) through multichip communications. The BS sends the network data via the Internet to an application server.

There are two types of WSN, namely structured and un-structured WSNs [7]. Typically, structured WSNs have a small number of sensor nodes and they are easy to manage. Sensor nodes are placed deterministically, i.e., the place of each node is determined in advance. In unstructured WSNs, many sensors are deployed in an ad-hoc manner. Therefore, the resulting WSN is more difficult to manage.

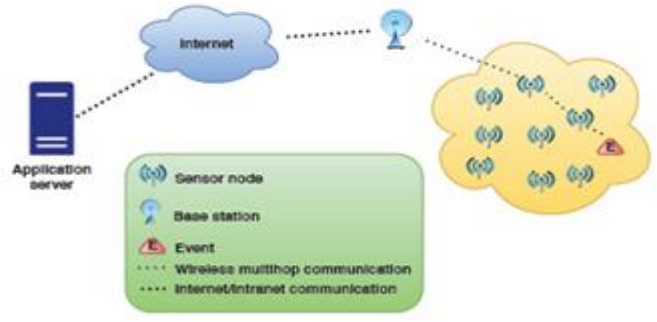

Figure 1: A wireless sensor network

The control of WSNs can be categorized into centralized, decentralized or distributed control which are depicted in Fig. 2. With centralized control, a single node has the global view of the network and decides whether the functionality of a node is required or not, i.e., the node should be active or not. With decentralized control, the nodes are divided into groups and there is a central node for each group. The interaction among the central nodes of all groups determines the activity of each node. In distributed control, there is no central control node and all nodes interact with each other for network-wide decision making, e.g., determining the active nodes for covering the network area.

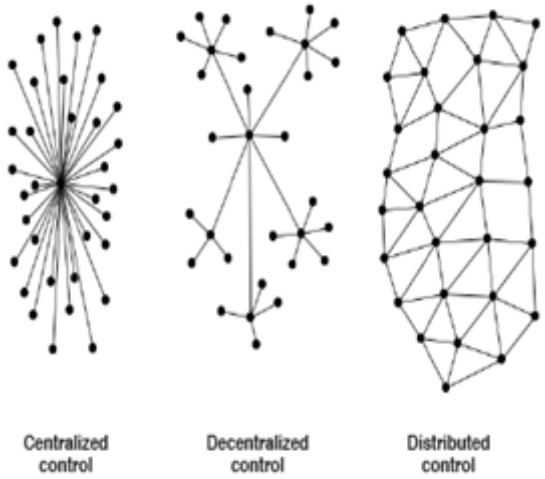

Figure 2: Different control types for WSNs

B. Typical Use Cases

There are several types of sensors such as acoustic, thermal, visual, etc. The survey in [8] reports that sensors monitor various ambient conditions. Examples are temperature [9], habit monitoring [10], movement detection [11], [12], humidity [13], military applications [14], oil and gas monitoring [15], health monitoring

C. Standards

The key design challenge for wireless sensor nodes is low power consumption. Standards for WSNs define sets of functions and protocols. Examples are IEEE 802.15.4,Zigbee, 6LoWPAN, and ISA100.11a. We briefly discuss them in the following.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

IEEE 802.15.4 is designed for low-rate wireless personal area networks (LR-WPAN). The main goals of this standard are low-cost implementation, low complexity, and low power consumption. The Physical layer of this standard supports bands between 868/915 MHz and 2.4 GHz. IEEE 802.15.4 is designed for short-range communication applications that require lowTransmissionpower. In these applications, maximizing the residual power of sensors is the mainchallenge.ZigbeeoperatesontopofIEEE802.15.4.Thi sstandard supports networks with a large number of sensors (i.e., up to 65k nodes). Sensors can monitor the environments for years thanks to low cost and low power features provided by Zigbee standard.

6LoWPAN (IPv6-based Low power Wireless Personal Area Networks) enables IPv6 over IEEE 802.15.4. In this standard, low power sensors can communicate with IPv6 speaking devices. An adaptation layer accommodates IPv6 packets into IEEE 802.15.4 frames. 6LoWPAN is mostly leveraged in embedded devices which are used in home and building automation or health-care automation.

D.Research Challenges

Asdiscussed,sensordevicessufferfrommanyresourceconst raints such as low power transmission and low batterypower. These devices are mostly used for tracking and monitoring applications such temperature, noise, etc. Therefore, a varietyofhardwareplatformsareneededtofulfillthemonitor ing and tracking goals. Here, we focus on research challenges that are performed on improving the nodes' efficiency in tracking and monitoring applications.

3. SDNBASICS

In this section, we briefly overview the concept of SDN and OpenFlow which is the most widely used for SDN in wireline networks.

A. Concept of SDN

SDN separates forwarding and control plane in communication networks. That means, forwarding nodes do not communicate with each other to populate their forwarding tables like in traditional networks, but a controller configures their forwarding tables. The Open Networking Foundation (ONF) [22] defines a three-level architecture for SDN which is illustrated in Fig. 3. It consists of an infrastructure layer, a control layer, and an application layer.

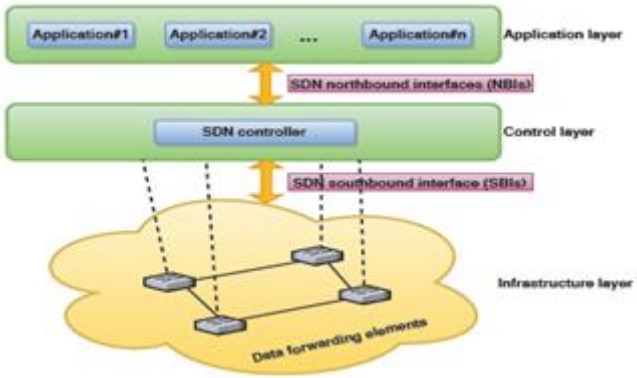

Figure 3: SDN architecture

i) Infrastructure layer: The infrastructure layer is the bottom part of the SDN architecture. It comprises a set of forwarding nodes such as switches, routers, access points, etc., which are often called forwarding elements or datapaths.

ii) Control layer: The control layer includes a set of controllers which control the datapaths through a so-called southbound interface (SBI) whose traffic is usually carried over a secured connection, e.g., over Transport Layer Security (TLS). The most-widely utilized SBI is Open-Flow. The controllers have an overview of the network, compute suitable forwarding behavior of all datapaths, and configure them with appropriate forwarding rules. Moreover, controllers can obtain information from forwarding elements, they may be triggered by so-called network applications, and in case of multiple controllers, they may communicate with each other.

iii) Application layer: The application layer comprises a set of network applications that are input to the controllers to install appropriate rules on the datapaths. Examples of network applications are routing, port

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

filtering, load balancing, network address translation, etc. Thus, the application plane defines policies which are translated by controllers into specific southbound instructions to control the forwarding behavior of network devices. Logically, the application plane communicates with the control plane over a northbound interface (NBI), but often the application plane consists of subroutines within a controller.

B. OpenFlow

OpenFlow [23], [24] is ais an architecture and a SBI forSDN which has been developed at Stanford University. Each OpenFlow switch has flow tables that can hold mostly a moderate number of flow rules (aka flow entries). They consist of match fields, counters, and actions. The match fields can refer to selected packet header fields like source/destination MAC/IP address and port, etc., i.e., the match fields extend over several protocols. Counters may be used to gather management information that can be leveragedby the controller. Examples for actions are forward, drop, modify, send to controller, etc. When a forwarding element receives a packet, it may be matched by a flow rule in the flow table. In that case, the specified counters and actions are applied to the packet.

The flow rules are installed by controllers on the forwarding elements. If no flow rule matches the header of an incoming packet (table miss), the behavior of the datapath depends on configuration. It may either drop the packet or send a packet digest to the controller to request the installation of another flow entry. The controller then computes new flow entries respecting the policies provided by the application plane and installs them on the requesting datapath and possibly also on others.

4. SD-WSN

In this section, we give an overview of SD-WSN. We first describe the general architecture of SD-WSN and explain its differences to non-software-defined WSNs. Then, we compare of SD-WSN and wireline SDN and finally we give an overview of software tools of SD-WSNs.

A. Architecture of SD-WSNs

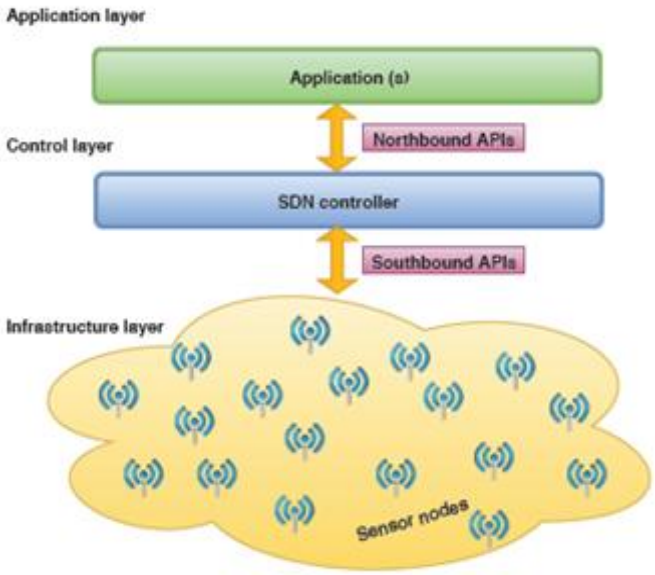

Figure 4: The General architecture of SD-WSNs.

Fig.4 shows the general architecture of SD-WSNs. The architecture consists of the following logical planes: i) data plane, ii) control plane, and iii) application plane.

The infrastructure layer of SD-WSNs includes a set of sensor nodes which sense and forward data in the network. The control layer includes the controller which controls the whole network. The application layer of SD-WSNs includes diverse applications of WSNs such as routing.

B. Difference to non-SDN based WSNs

In non-SDN based WSNs, to obtain the topology of thenetwork, topology discovery mechanisms are required. They rely on broadcast messages which periodically are sent by each node within its transmission range to identify the neighbors. This operation adds a significant overhead to the network and it also consumes a lot of energy. After obtaining the network topology, several decisions can be made for the network, e.g., routing decisions to steer the network traffic. To perform thesedecisions each node needs to store routing tables within its limited memory and computes the path for other nodes

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

C. Comparison of SD-WSN and Wireline SDN

Applying SDN to WSNs introduces a number of new research challenges which make them different from wireline networks. In this section, we give an overview of these new challenges. Network management in WSNs is different from other networks. In WSNs the main goal is to minimize the energy consumption.

D. Standardization Efforts

The standards of SD-WSNs should define the set of functions and protocols for sensors and controllers. The authors of [33] used IEEE 802.15.4, to build sensor nodes that can be leveraged in an SD-WSN. This standard is not confirmed by any standardization community. There is no formal standard for SD-WSNs

E. Software Tools

In this section, we give an overview of software tools for SD-WSNs. We concentrate on open-source tools which are freely available and can be exploited.

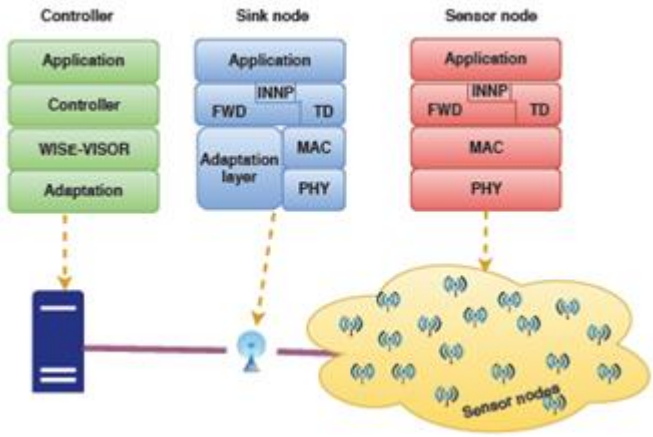

Figure 5: SDN-WISE architecture and protocol stack

a) Architecture: The SDN-WISE architecture has threedifferent components: sensor node, sink node, and controller. Fig. 5 illustrates the general architecture of SDN-WISE and the protocol stack of each component. We describe each of them in the following.

Each sensor node in Fig. 5 has the following layers inits protocol stack: i) Application, ii) In-Network Packet Processing (INPP), Forwarding, and Topology Discovery (TD), iii) Media Access Control (MAC), and iv) Physical.

b) Flow Table: Tab. I shows an example of the WISEflow table of SDN-WISE and we explain the structure of the table without stating the detailed values. A WISE flow table consists of matching rules, actions, and statistics.

c) Software Simulation Tool: SDN-WISE offers functionalities similar to Mininet [34]. Mininet is a widely used network simulator to perform campus-size network experiments. It uses Cooja [35], which is a network simulator for Contiki OS, which is the operating system for low-power wireless Internet of Things [36], to create the network. Fig. 6 shows a running example of an SD-WSN with 17 nodes in SDN-WISE, which is randomly deployed in a two-dimension network area. Node 1 is the sink node in this figure SDN-WISE defines an open-source controller which performs the routing decisions among the deployed nodes based on Dijkstra's algorithm. The nodes collaborate with the controller through sink node.

d) SDN-WISE Features: SDN-WISE supports duty cycle, i.e., the possibility of periodically turning off the radio interface of each node and its data aggregation. SDN-WISE handles the packets based on the information in its payload and its header section.

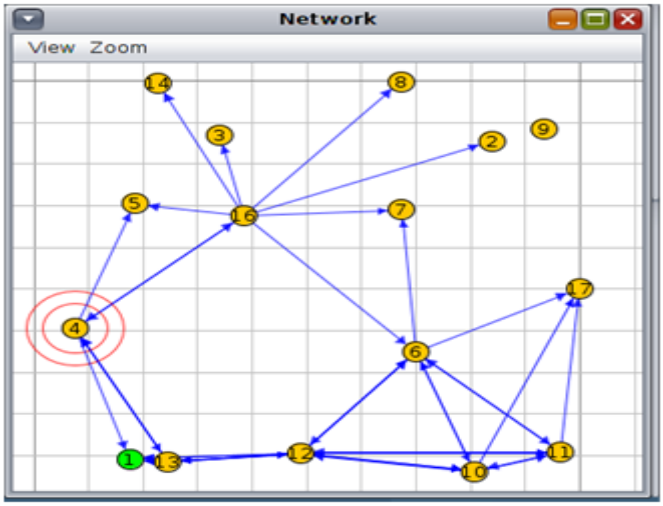

Figure 6: A sample network in SDN-WISE.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A sensor node isshown with a numbered circle and the communication links between the nodes are depicted with lines. The direction of the link shows transmission direction.

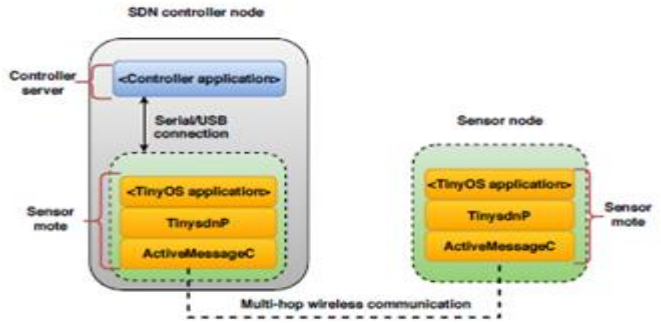

Figure 7: Layers of Tiny-SDN components.

The SDN controller node performs traffic flow management. It has two main components: Sensor mote module which is responsible for communicating with other sensor motes using ActiveMessageC. Each sensor mote module was shown as an instance of a sensor node in Fig. 7, and Controller server module which hosts the controller application and managesthe network flows and the topology information.

5. ADVANCES IN WSN THROUGH SDN

In this section, we overview SDN-based approaches for WSNs and classify the research literature in several categories. Fig. 8 depicts the organization of the reviewed works in this section.

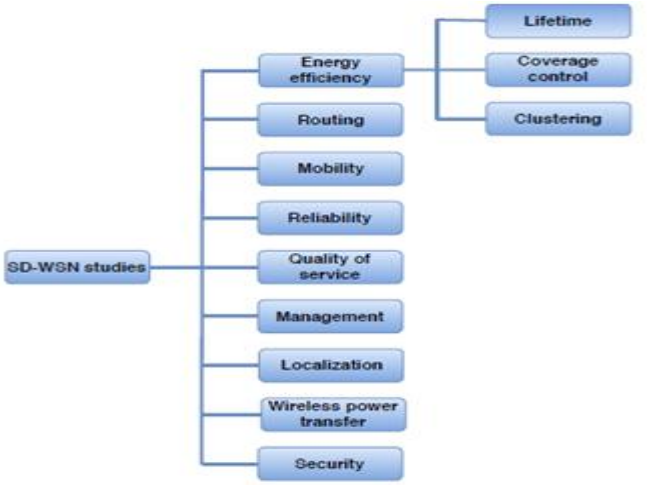

Figure 8: Categorization of SD-WSN studies.

A. Energy Efficiency: Energy-efficiency is one the most critical aspects of WSNs and it is the objective of many WSNs research works. Sleep scheduling approaches can be leveraged to switch the nodes into idle state if their functionality is not required. These algorithmscan be used to reach the networks' goal.For instance,the authors of used sleep scheduling approach to extend the network lifetime while keeping the connectivity of nodes and preserving the coverage requirements. Here, we classify the energy-efficient works into three areas: lifetime, coverage control, and clustering.

1) Lifetime: Prolonging the network lifetime gives thepossibility to utilize the nodes functionalities for a longer period of time. For example, computational tasks like path selection and neighbor discovery consume most energy in WSNs. The energy consumption to send a single bit of data by a sensor in a WSN, e.g., composed of MICA motes, is at least 480 times higher than performing one additional 32-bit instruction by CPU. The authors ofstated that data transmission consumes approximately 80% ofnodes' power.

2) Coverage Control: Coverage is one of thewidely used applications of WSNs in which a network area or a set of targets should be covered by the sensor nodes in the network [12]. Coverage control activates or deactivates the sensor nodes to cover a network region. Network coverage can be categorized into: target, area, and barrier coverage. The goal of target coverage is to cover a set of stationary or moving targets while in the area coverage the goal is to monitor the whole network area.

Fig. 9 shows two different coverage problems in WSNs. For example, Fig. 9a illustrates a network that the deployed nodes were exploited to monitor the whole network area while Fig. 9b shows a networkso that the sensor nodes should monitor a set of targets. One common approach to the area or target coverage is to use a subset of nodes to monitor the network coverage requirements.This technique is also known as cover-set approach.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

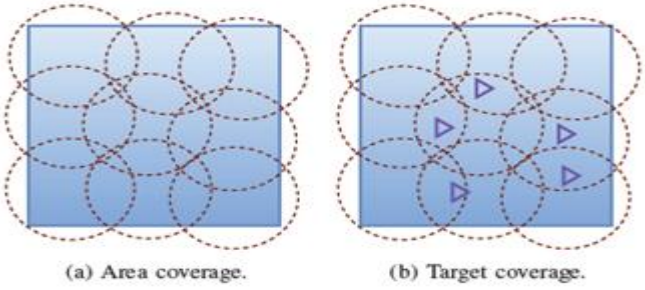

Figure 9: Coverage control examples

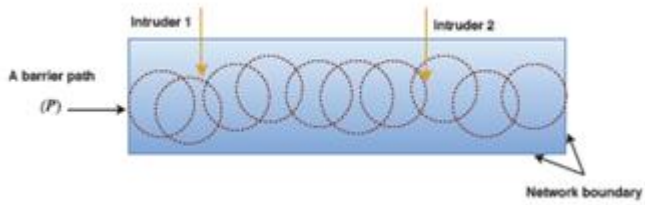

Figure 10: An example of barrier coverage with two intruders and a barrier path (P) which can detect any penetration to the network.

3) Clustering: Clusteringis widely used in WSNs for controlling the energy consumption of nodes and for routing. Clustering puts the nodes into clusters and there is a head node for each. Cluster heads (CHs) are in charge of collecting data from the nodes in their clusters and sending them to the BS while non-CH nodes are responsible for gathering the network information and forwarding it to the CHs [62]. The idea is to select the most powerful node as a CH to transfer the network data to sink node. Therefore, selecting suitable CHs is a challenging issue which was considered by researchers. Fig. 11 shows an example of a clustered network with three clusters. Each cluster member is connected to the sink node through its CH.

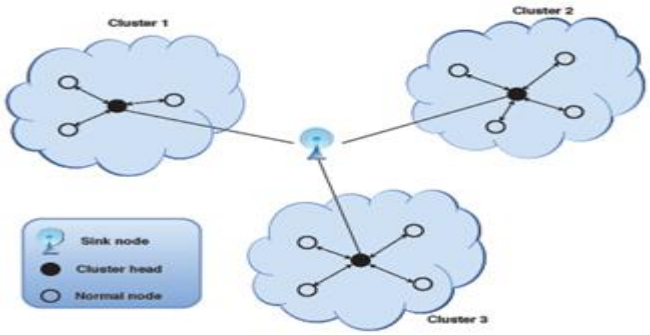

Figure 11: A clustered WSN with three clusters.

Clustering in SD-WSN with the aim of reaching energyefficiency was studied in [63], [64]. In this work, the SDN controller collects information of the network topology via Link Layer Discovery Protocol (LLDP) and installs suitable rules to gather the statistics of the nodes. The SDN controller is co-located in CH in the proposed architecture to take the control of all nodes in the cluster. The SDN controller can install a suitable rule on each flow table of the nodes to gather the information and send them via the controller to sink node. There are more than one controller and they can interact with each other to meet the global goal of the network.

B. Routing: There are many routing protocols for WSNs. The works in, provide a survey on routing challenges and design issues in WSNs. Transferring the network data efficiently is one of the main critical challenges in WSNs. Objectivespursued by routing protocols are: congestion control, delay minimization, throughput maximization, etc. The routing can be performed packet or flow-based.

C. Mobility: Mobility in WSNs can be classified into weak and strong mobility. Weak mobility results from changes of the network topology. For example, nodes in WSNs are prone to failure for many reasons such as hardware or battery problems. Therefore, they have to be replaced by new nodes. Strong mobility results in physically moving the place of nodes.

D. Reliability: Reliability of WSNs includes the reliability of several components such as node and link. For example, the reliability of a node includes the reliability of battery, radio, hardware, middleware, operating system, and application. In WSNs, the monitored data is transferred to the outside of the network via multi-hop connections. Any failure in the network causes energy consumption due to sending traffic through non-energy efficient paths. For instance, the objective of reliable routing algorithms is to maximize the packet delivery ratio.

E. Quality of Service (QoS): QoS provisioning deals with challenges that offer a guaranteed level of service delivery to a network. QoS requirements can be specified into congestion, packet loss, bandwidth, and jitter. Providing QoS is different among applications

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

because various requirements such as loss and delay could be planned for a specific application. For example, real-time applications are sensitive to delay rather than loss, while for other applications like target tracking reliable and timely delivery data is important. QoS provisioning can be performed per-packet or per-flow.

F. Management: Network management in WSNs is a challenging process including network configuration, provisioning, and maintenance. Managing a network with different nodes from different vendors requires a complex management process. The management mechanisms allow the network administrators tomanage vendor-specific nodes in WSNs.

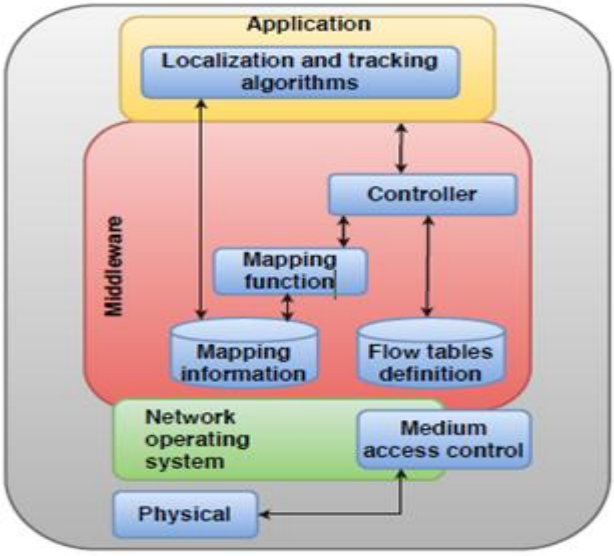

Figure 12: Base station architecture in Smart

The Middleware layer has the following components: controller, flow table definition, mapping function, and mapping information. The mapping function creates a network map based on the received table from the neighbor sensors and can be directly invoked from the controller if needed. The network mapping information, e.g., energy consumption, response time, link quality, is stored in a database and can be invoked at anytime. The application layer defines specific functionality to each node based on its available physical features, e.g., temperature monitoring, and contains a location component which is also denoted as Localization and Tracking Algorithms (LTA).

The authors proposed a distributed control system to manage the nodes in SD-WNSs. To distribute the controllers in the network, a fragmentation mechanism is leveraged whichaims at placing the controllers close to the network devices to improve the energy efficiency of the network. A radio resource allocation mechanism in SD-WSNs is proposed. The controller of SD-WNS dynamically assigns the suitable radio resource to each node. The authors modeled the problem asan optimization problem with QoS constraints to minimize the energy consumption of the nodes.

G. Localization Location information of each node is necessary for many applications of WSNs. Typically, the nodes are randomly scattered in the network zone.Localization techniques aim at positioning each node. Global Positioning System (GPS)is widely leveraged for this purpose, but it requires more energy to run and it is not easy to install this system on board of each node.

The authors modeled the localization problem inSD-WSNs based on 0-1 programming problem and proposed an SDN-based localization algorithm to select the nodes in localization mechanism. There are two types of nodes in this architecture which are called agent and anchor nodes. The agent nodes, with their exact location, were exploited to find the location of anchor nodes. The SDN controller interacts with agent nodes in the localization process.

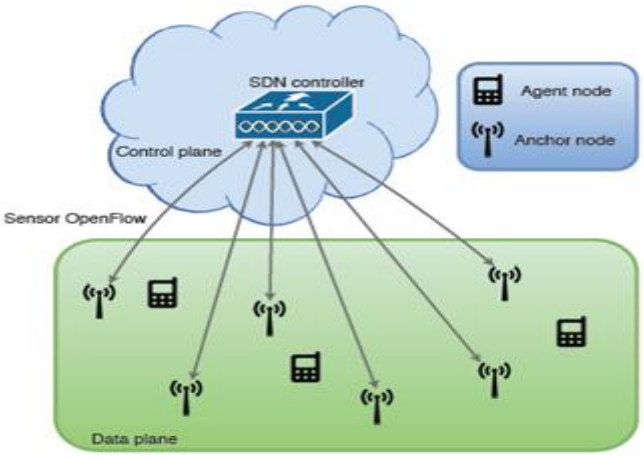

Figure 13: Node localization example in SD-WSNs

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An anchor-based scheduling algorithm for positioning the nodes in heterogeneous SD-WSNs was proposed. The SDN controller determines the position of each anchor node based on the network power constraints. Fig. 13 shows a sample architecture for localization in SD-WSNs. The SDN controller interacts with agent nodes through Sensor- OpenFlow in localization process.

H. Security: Security is one of the critical challenges in WSNs. The authors surveyed the security challenges of WSNs

The authors classified the main threats on SDN-based networks as follows.

i) Traffic flow attacks can be performed on forwarding elements and controllers. The malicious user launches DoS attacks to devastate the resource of network devices. This threat can be mitigated by authentication mechanisms.

ii) Forwarding device attacks could be used on each forwarding element to drop, slow down, or discard the network traffic. This attack can be also exploited to inject traffic to overload the controller.

iii) Control plane communication attacks can be performed as DoS attack for data theft in the network. Leveraging common secure communication protocols such as TLS or secure sockets layer (SSL) are not enough to avoid those attacks because there are several man-in-the-middle attacks for the TLS/SSL model.

iv) Controller attacks compromises the controller to obtain the control of entire network. Using intrusion detection systems is not enough due to the difficulty in finding the exact combinations of events to construct this attack.

v) Lack of trust between applications and the controller is similar to control plane communication attacks because a trusted communication between network applications and the controller cannot easily be established. Certifying the forwarding devices is different than certifying of applications.

vi) Administration stations attacks. The devices in administration station are used to access the controller in SDNbased networks. Indeed, using the administration stations to control the network devices are also common in other networks. The difference is that each machine in the administration station can be exploited to program the network from a single point if the attacker compromises the controller.

vii) Lack of trusted resources for forensics and remediation. There are resources in a network that can be leveraged for troubleshooting. Such reliable information are necessary to investigate the facts of incidents in the network and without them, it is difficult to find a remedy for a problem. This is not specific to SDN networks.

I. Wireless Power Transfer: The power transfer problem in SD-WSN was studied with aiming at real-time recharging of sensor nodes. In this work, the SDN controller is in charge of finding an optimal position for the energy transmitters. Also, it can determine the minimum number of energy transmitters over the course of primary process to prolong the charged energy by each node in the network.

Additionally, the controller can fairly distribute the energy among all the nodes by having the workload information of each node. The authors proposed different methods for maximizing the charged energy and fairly distributing the energy among all nodes. For this purpose, they formulated as an optimization problem with several constraints and proposed a solution. The controller is in charge of selecting energy transmitters to balance the energy consumption of the nodes.

J. Comparison of SDN-based and non-SDN based WSNs:

In this section, we compare SDN-based and non-SDN based works in WSNs. One of the main advantages of exploiting SDN in WSNs is energy saving. As discussed in Sec. V-A, sending broadcast messages is mandatory for topology discovery. While in the SDN-based WSNs, this process is performed by the controller, which save energy for each node. For instance, in the scenarios like localization and wireless power transfer, the SDN

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

controller can easily locate the best places for the nodes. Tab. IX summarizes the differences between SDNWSNs and non SDN-based WSNs.

6. CHALLENGES IN SD-WSN

In this section, we discuss open challenges in SD-WSNs. A. Network Operation:We discuss the network operation challenges that require further investigation in SD-WSNs.

1) Re-Clustering: In non-SDN based WSNs, cluster heads deplete their energy due to the high number of communications they have with other nodes within the cluster and with other cluster heads to transfer the network data. New cluster heads need to be selected to steer the network traffic. Cluster head nodes in SD-WSNs inherit the same characteristic of WSNs.Therefore, this challenge needs to be considered in SD-WSNs. SD-WSN may be able to achieve faster and better re-clustering which has not yet been studied.

2) Topology Control: Controlling the network topology can improve energy efficiency of the network. The primary objective of any topology management system is to maintain the network coverage while keeping the nodes connected.

3) Node Mobility: Sensor nodes may intentionally change their positions. That can improve the WSNs capabilities in many aspects such as automatic node deployment, rapid reaction to event changes, and flexible topology management.

4) Improving Routing: Routing can be improved in SDWSNs by leveraging the controller which has the global overview of the network and of the devices status. For example, a routing path may have several constraints like reliability. Moreover, other constraints such as bandwidth and delay can be considered. This issue can be modeled as Multi- Constraint Optimal Path (MOCP) problem.

5) Data Traffic Scheduling: Sensor nodes are exploited to gather environment data. After collecting the data from all or some nodes, they should be forwarded to a BS. This can be performed by a collaboration among the nodes in a WSN.

6) Network Monitoring: Network monitoring checks theFunctionality of network devices through specialized management tools. It ensures the availability and the performance. WSNs are typically deployed in a complex and distant environment to monitor objects without human interactions.Wireless links are not stable and prone to packet loss. Additionally, nodes can fail during the network operations. Thus, real-time monitoring tools are required to check the operations of the nodes in the network.

B. Challenges for Network Applications: Network applications can benefit from SDN in WSNs. Westate the research challenges for WSN applications such as coverage and node mobility that require investigation in SDWSNs.

1) Coverage: Some of coverage issues in SD-WSNs are currently studied in the literature. However, several aspects of coverage problem in SD-WSNs need further investigation. We overview them in the following.

a) Partial Coverage: The goal of area coverage is tocover the whole network area by the nodes.

b) Coverage Holes: Coverage algorithms may lead to having coverage holes. A coverage hole is the amount of the network area that is not covered either by the nodes or the chosen active nodes. Fig. 14 demonstrates a sample network in which the deployed nodes lead to a coverage hole. In this figure, the network area is divided into fixed-size cells,which is one of the common ways to compute the coverage contribution of each node. This is not easy to perform in non-SDN based WSNs because the network area information is required and it should be distributed among the nodes to check.

This issue needs further investigations in SD-WSNs.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

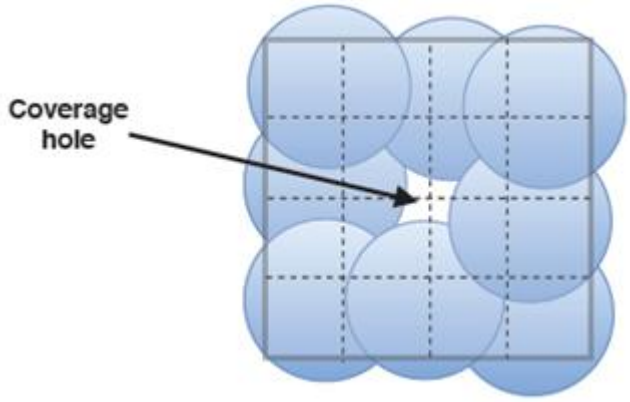

Figure 14: An example of coverage hole.

2) Leveraging Node Mobility: To improve the nodes'functionality in covering the network region, the nodes' mobility can be leveraged. For example, coverage holes can be covered by moving the nodes toward the coverage hole area. This problem needs investigation in future SD-WSNs works.

C. SDN-Specific Challenges

In this section, we describe the challenges that are specific to SDN networks and applying SDN to WSNs inherits the same issues.

1) Control Plane Resilience: In an SD-WSN, a singlecontroller can be a single point of failure for the network. Multiple controllers can be leveraged to overcome the controllers' failure.The authors studied the controller failure by adding an extra controller, but still, the inter-communication mechanism between controllers are not considered in this scenario. A complete solution is needed to handle controller failures in SD-WSNs.

2) Data Plane Resilience: In SDN network, the controller is in charge of detecting data plane failures and it the case link or node failures, packets can no longer be forwarded to affected next hops. The controller repairs the path by installing new flow entries in wireline SDN. Fast rerouting (FRR) has been introduced for fast and local reaction without controller intervention. This may also be adopted for SD-WSNs.

3) Scalability: Scalability is one of the most challengingproblems in SDN-based networks. The robustness of the network was studied in, but it suffers from scalability issues, which has also to be considered in SD-WSNs. Utilizing several controllers in the network solves the problem but it opens the problem of optimal controller placement.

D. Security: Many WSNs have mission-critical responsibilities such as military applications. Therefore, security needs to be taken into account in designing the network for such applications. Due to the nature of WSNs, security issues are more complicated than in other network types. The threats and vulnerabilitiesfor SDN-based WSNs are identified in Sec. V. There is a need for suitable solutions for each of those threats in the future works. Most of current SDN security solutions are adapted for switches and routers.

7. LESSONS LEARNED

We summarize some insights gained during the preparationof this survey.Sensor nodes have only a limited battery, which constrainstheir lifetime. Therefore, energy saving is an important goalin most WSNs. This is mostly achieved by adapting the communicationrange of sensor nodes. The communication rangeaffects the resulting topology and impacts the managementof the WSN. The sensing range impacts the coverage areaof a node, which is important as most WSNs have beendeployed for environmental monitoring. As the adaptation ofcommunication range influences significantly the operation ofa WSN, it is a difficult task. We believe that it can be bettersolved by a powerful server with a central view on the networkthan in a distributed way. Moreover, distributed control ofWSNs by itself causes lots of communication overhead so thatthe communication of sensor nodes with an SDN controllermay save energy. As offloading energy- and communicationhungrytasks to a powerful controller can significantly extendthe lifetime of sensor nodes, WSNs may particularly benefitfrom SDN. However, there are some challenges to solve.

So far, there is not yet a standardized architecture for SDWSNand appropriate hardware is missing. There are

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

somesimulation tools for SD-WSN, but no testbeds such as Mininet that allows running multiple real nodes on a single machine sothat experimentation with SD-WSN requires more effort thanin wireline SDN. Data plane and control plane resilience arepartially unsolved problems in wireline SDN, which also holdsfor SD-WSN. When managing a WSN, topology, routing,and various applications need to be jointly optimized, and reclusteringactions may be needed to balance the battery of all nodes. These are demanding tasks even for a central controlserver and appropriate control strategies are needed. Finally, security in SDN is not fully understood, which is certainly an even bigger problem for SD-WSN as sensor nodes may be even more exposed to potential attackers. Below the line, we believe that the benefits of SDN outweigh potential drawbacks and see SD-WSN as a promising research area.

8. CONCLUSION

This survey gave a brief overview of WSNs and SDNand introduced the concept of software-defined WSNs (SDWSNs) including their operations, e.g., topology discovery and routing decisions, that are different from WSNs. Coordination of distributed nodes and energy efficiency are the most important challenges in WSNs. In non-SDN based WNSs, they are mostly solved in a distributed manner. SD-WSNs favor central control. That may save energy because redundantcommunication can be avoided, energy-constraint nodes can be offloaded from energy-efficient task by moving them to the controller, and application-specific goals may be achieved with fewer active nodes through more intelligent operation. We reviewed advances for WSNs through SDN and challengesfor SD-WSNs that should be solved in the future. Finally, we pointed out lessons learned during the preparation of this survey.

REFERENCES:

[1] N. Mckeown, How SDN will shape networking (Oct. 2011). URL http://www.youtube.com/watch?v=c9-K5O qYgA.

[2] The Open Networking Foundation, Software-defined networking (SDN) definition (retrieved: Jan 2017). URL https://www.opennetworking.org/sdn-resources/sdn-definition

[3] H. I. Kobo, A. M. Abu-Mahfouz, G. P. Hancke, A survey on softwaredefined wireless sensor networks: Challenges and design requirements, IEEE Access 5 (2017) 1872–1899.

[4] M. Ndiaye, G. P. Hancke, A. M. Abu-Mahfouz, Software defined networking for improved wireless sensor network management: A survey, Sensors 17 (5) (2017) 1031.

[5] N. A. Jagadeesan, B. Krishnamachari, Software-defined networking paradigms in wireless networks: a survey, ACM Computing Surveys (CSUR) 47 (2) (2015) 27.

[6] I. T. Haque, N. Abu-Ghazaleh, Wireless software defined networking: A survey and taxonomy, IEEE Communications Surveys Tutorials 18 (4) (2016) 2713–2737. doi:10.1109/COMST.2016.2571118.

[7] H. M. Ammari, A. Shaout, F. Mustapha, Sensing coverage in threedimensional space: A survey, Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures (2016) 1.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: A survey, Comput. Netw. 38 (4) (2002) 393–422. doi:10.1016/S1389-1286(01)00302-4.

[9] L. Yu, N. Wang, X. Meng, Real-time forest fire detection with wireless sensor networks, in: Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005., Vol. 2, IEEE, 2005, pp. 1214–1217.

[10] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, J. Anderson, Wireless sensor networks for habitat monitoring, in: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, ACM, 2002, pp. 88–97.

[11] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, et al., A line in the sand: a wireless sensor network for target detection, classification, and tracking, Computer Networks 46 (5) (2004) 605–634.

[12] H. Mostafaei, M. Shojafar, A new meta-heuristic algorithm for maximizing lifetime of wireless sensor networks, Wireless Personal Communications 82 (2) (2015) 723–742. 15

[13] D. Ye, D. Gong, W. Wang, Application of wireless sensor networks in environmental monitoring, in: Power Electronics and Intelligent Transportation System (PEITS), 2009 2nd International Conference on, Vol. 1, IEEE, 2009, pp. 205–208.

[14] S. H. Lee, S. Lee, H. Song, H. S. Lee, Wireless sensor network design for tactical military applications: Remote large-scale environments, in:
Military communications conference, 2009. MILCOM 2009. IEEE, IEEE, 2009, pp. 1–7.

[15] V. Jelicic, M. Magno, D. Brunelli, G. Paci, L. Benini, Contextadaptive multimodal wireless sensor network for energy-efficient gas monitoring, Vol. 13, IEEE, 2013, pp. 328–338.