# An Overview on Programming Characterize Remote Sensor Arrange Challenges:Wireless Sensor Network.

Prof. Devidas S. Thosar[#1], Ankita Gaikwad[#2]

[#1]*Assistant Professor, Computer Department,* [*2]*M.E Student, Computer Department,*
*S.V.I.T, Chincholi, Nasik, Maharashtra, India.*

[1]devidas.svit@gmail.com

[2] 2013ankitagaikwad@gmail.com

*Abstract —*
*Wireless Sensor Networks (WSN), an element of pervasive computing, are presently being used on a large scale to monitor real-time environmental status. However these sensors operate under extreme energy constraints and are designed by keeping an application in mind.While it has been a belief for over a decade that wireless sensor networks (WSN) are application-specific, it can lead to resource under utilization and counter-productivity in wirelesss sensor network. We also identify two other main problems with WSN: rigidity to policy changes and difficulty to manage.Network virtualization is a promising technology that enables the deployment of multiple virtual networks over a single physical network. These virtual networks are allowed to share the set of available resources in order to provide different services to their intended users.To achieve a widespread deployment of Software-Defined Networks (SDNs) these networks need to be secure against internal and external misuse. Yet, currently, compromised end hosts, switches, and controllers can be easily exploited to launch a variety of attacks on the network itself.However these sensors operate under extreme energy constraints and are designed by keeping an application in mind. Designing a new wireless sensor node is extremely challenging task and involves assessing a number of different parameters required by the target application, which includes range, antenna type, target technology, components, memory, storage, power, life time,security, computational capability, communication technology, power, size, programming interface and applications. This paper analyses commercially (and research prototypes) available wireless sensor nodes based on these parameters and outlines research directions in this area.*

Keywords ***—Software defined wireless sensor networks, software defined networking, wireless sensor networks.Wireless Sensor Network (WSN), FPGA,sensor node, Active Node, CCU.Software-defined networking, OpenFlow, wire-less sensor networks.***

## I.INTRODUCTION

The wireless sensor networks has given to the development of smart sensors in recent years. Wireless sensor networks (WSN) consist of micro-sensors capable of monitoring physical and environmental factors such as temperature, humidity, vibrations, motions, seismic events, etc. The sensor nodes are small, inexpensive, and intelligent [1] owing to the drastic improvement in Micro Electrical Mechanical Systems (MEMS) development. The emergence of the Internet of Things (IoT) paradigm has augmented the scope of WSNs demand, further cultivating the ongoing research in this field. IoT is a network of smart objects interconnected through a communication medium [2]. WSNs are expected to play a significant role in IoT, since the sensor nodes are the main building blocks of this concept [3]. An estimated 50 billion devices are envisioned to be connected to the network by 2020 [4], and most of them will be equipped with sensors and actuators. Thus WSNs will be pivotal to the efficacy of IoT.In the last few years wireless sensor networks(WSNs) have drawn the attention of the research community, driven by a wealth of theoretical and practical challenges. This progressive research in WSNs explored various new applications enabled by larger scale networks of sensor nodes capable of sensing information from the environment, process the sensed data and transmits it to the remote location WSNs are mostly used in, low bandwidth and delay tolerant, applications ranging from civil and military to environmental and healthcare monitoring.

Another problem with WSN is that they are rigid to policy changes. Policies are rules related to network-exogenous factors such as business operation and user access, as opposed to network-endogenous factors such as node and link properties which have been extensively studied over the years and handled algorithmically.Recent technological

developments and changes in usage trends have created increasing demands on spectrum bands. On the other hand, spectrum utilization measurements indicate that the reserved spectrum bands are not fully utilized by its licensed users (Primary Users (PUs)). A PU pays licensing fees for reserving a part of the spectrum (divided into a set of channels) for its transmissions and no one else has the authority to use this part. PUs utilization of the reserved spectrum is bursty in nature and varies greatly over time. It is also different for different channels and different geographic locations.Cyber attacks are increasingly becoming more complex and are major concerns for users, corporate organizations and governments. As a relatively recent proposal, Software-defined Networking (SDN) has not yet matured towards mitigating such attacks. In fact, currently, end hosts, switches and controllers are prone to attacks, a situation that has severe implications: i) end hosts and switches can be misused to launch Denial-of-Service (DoS),link fabrication, or man-in-the-middle attacks and ii) worse, a faulty or malicious controller can reprogram the entire network for instance for the purpose of data theft in data centers.

## II. Literature Survey

Software defined networking (SDN) is a new networking paradigm that aims to simplify network management and configuration. SDN offers a complete paradigm shift from traditional networking. It seeks to greatly improve network efficiency through high level novel abstractions. SDN decou-ples the network intelligence, the control plane, from the packet forwarding engine, the data plane. The separation enables a provision of centralized network intelligence at the controller, which has a global view of the network. SDN introduces benefits such as vendor independence ,het-erogeneous network management, reliability and security not possible in traditional networks. While SDN was initially earmarked for large-scale enterprise networks, it has the potential to impact on any networked system. The rest of this section briefly discusses some of the major aspects of SDN, namely the architecture, protocols, standards, applications and security.Sensor networks are becoming more popular in applications related to environment monitoring to structural health monitoring and today a number of research teams are developing efficient nodes for such smart networks capable of processing data at node end before transmitting to base station, having compact size, reduced power consumption,low cost and most important minimum human ntervention. In this section we outline some of this related work.One of the prime examples of such sensor network is a project named “Smart-Dust” carried out by University of California at Berkeley, USA.The main objective of the project was to develop a compact size node that includes sensor, capability to compute the sensor data onboard, low cost, minimal power consumption and having bidirectional wireless communication capability. Another interesting research testbed was the,which integrated the functionality of Mica onto a single 5 mm 2 chip. A micro-radio is duilt by spec, an analog-to-digital converter, and a temperature sensor on a single chip in wsn, which lead to a 30-fold reduction in total power consumption.The integrated RAM and cache memory architecture greatly simplified the design of the mote family.The footprint also requires in tiny os a specialized operating system in wsn, which was developed by UC Berkeley. The combination of Motes and TinyOS is gradually becoming a popular experimental platform for many research efforts in the field of WSNs.

## IV.Proposed System

Software defined networking (SDN) is a new networking paradigm that aims to simplify network management and configuration. SDN offers a complete paradigm shift from traditional networking. It seeks to greatly improve network efficiency through high level novel abstractions. SDN decouples the network intelligence, the control plane, from the packet forwarding engine, the data plane. The separation enables a provision of centralized network intelligence at the controller, which has a global view of the network.

SDN introduces benefits such as vendor independence, heterogeneous network management, reliability and security notpossible in traditional networks.

While SDN was initially earmarked for large-scale enterprise networks, it has the potential to impact on any networked system. The rest of this section briefly discusses some of the major aspects of SDN, namely the architecture, protocols, standards, applications and security.wireless sensor node is based on a transceiver operating in the 2.4 GHz ISM band. The node was initially thought of as an active RFID tag for monitoring temperature in goods. However, it has been shown that it is also possible to use it as a wireless sensor network node. The node is equipped with an extremely low power microcontroller (Microchip PIC16F87), for executing communication protocols and sensor

The memory and processing resources are very limited to keep the price and energy consumption as low as possible. The node is also equipped with a temperature sensor.
Overall we can see that most of the research is focused on developing smart sensing nodes for WSN.Hence we studied the most important nodes in the current literature to see which application can be practical. The next section evaluates these nodes.

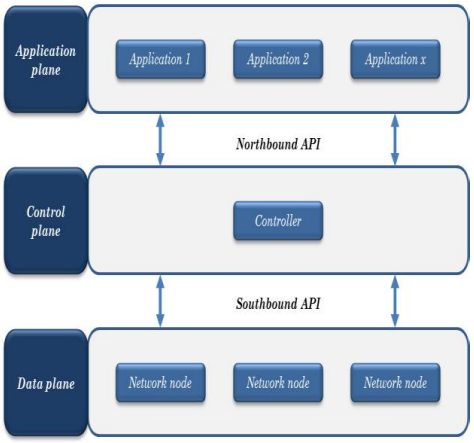


Fig 1.The basic SDN framework with the three planes and a central controller.

## IV.System Architecture

Traditional networks, which typically consist of routers andswitches as network devices; become difficult to monitor and upgrade as the network grows, thus stifling growth. Large networks also become heterogeneous due to the use of different proprietary protocols, which fundamentally means theyconsist of different network islands that only cooperate at lower levels of communication.

This makes it difficult to implement any policy changes, upgrades, and patches. Traditional networks are also mostly hierarchical,tree based and static, which leads to what most have termed ‘ossification’’ . Ossification refers to a phenomenon of conforming to the conventional way of networking where everything is coupled on the network device.

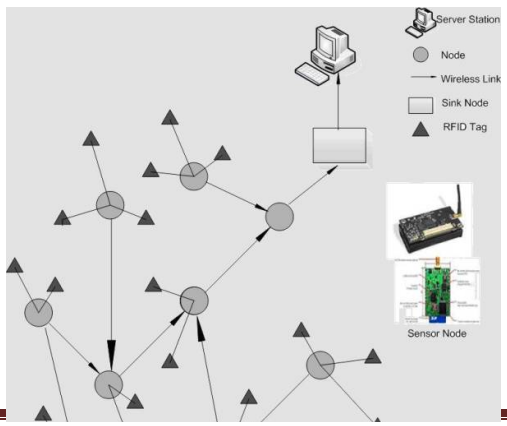


Fig 2. Wireless Sensor Network

WSN node is comprised of low-power sensingdevices, embedded processor, communicationchannel and power module. The embedded processor is generally used for collecting and processing the signal data taken from the sensors.Sensor element produces a measurable response to achange in the physical condition like temperature, humidity, particulate matter(e.g. CO 2 ) etc.

The wireless communication channel provides amedium to transfer the information extracted from he sensor node to the exterior world which may be acomputer network and inter-node communication. However, WSN using IEEE 802.15.4 Wireless Personal Area Network protocol (WPAN) or Bluetooth is complicated and costly [10, 18].Using RFID to implement wireless communication is relatively simple and cheap [6]. Zigbee protocol can also be used for communication; alternatively th RS232 standard for wireless transmission of data can be adopted because the data rate of RFID and that of RS232 is same in terms of bits per second (bps).

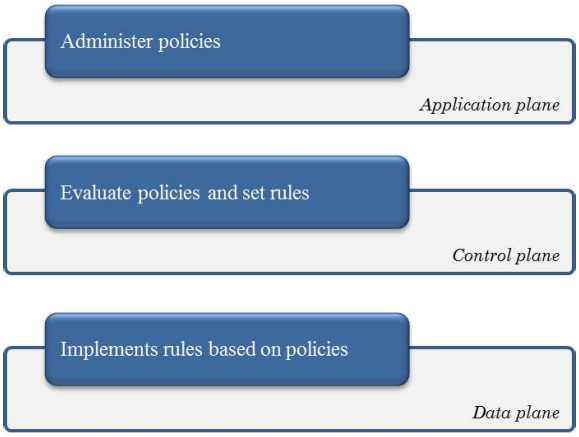


Fig 3. The context-aware and policy based routing model.

Initiation phase: sensor nodes connect to the controller using the Sensor OpenFlow protocol. The nodes also supply the controller with all relevant information such as node status, CPU load, etc.Topology discovery phase: The node supplies the controller not only with its own information but its neighbours’ as well. The controller forms a routing map table. The table has all the nodes and their next best hops. The route link has context information such as CPU load, service information and power levels of the next hop. Services are any policies defined for that route such as security, privacy, etc.
Decision phase: The controller uses a recursive destination based lookup algorithm to look for a route in the mapping table. Policy based route phase: The routes are chosen using defined policies. The

algorithm lookup will determine all available routes towards the destination and a particular route will be chosen if it matches the policy criteria, i.e. ignore any route with a CPU usage of at least 90%. Should all routes not match the policy, packets could be dropped.Enforcement phase: The controller enforces the routing onto the switch devices.

## V.LIMITATIONS

While designing a WSN the designer must pay ke attention to the life time of the entire networkbecause one of the main objective of WSN is to have minimum human intervention. Other than processing the communication part is considered to be the second largest energy consuming element of the node. The RF transceiver consumes most of the energy during the active state. Network lifetime can be increased by having nodes only operate their radios for brief periods of time.

## VI.CONCLUSION

In this paper presents the first effort that synergizes SDN and WSN to solve WSN-inherent problems. The proposed solution, SD-WSN with SOF, might provoke interesting discussions from the research community and open the door to a wide range of innovation opportunities. By that and ultimately, we expect to see a new generation of WSN that are versatile, flexible, and easy to manage. which is specify for particular image.

In this paper, we proposed a software defined virtualization based resource allocation framework for multi-cell CRNs. We ocused our study on providing a multi-layer approach to efficiently allocate resources with the goals of avoiding the co-existence problem, increasing resource utilization and network throughput and decreasing blocking rates and overheads.

## ACKNOWLEDGMENT

We take this opportunity to express our hearty thanks to all those who helped us in the completion of the project. We express our deep sense of gratitude to our internal guide Prof. D. S. Thosar, A PG Coordinator.,Computer Engineering Department, Sir Visvesvaraya Institute of Technology, Chincholi for their guidance and continuous motivation. We gratefully acknowledge the help provided by them on many occasions, for improvement of this project with great interest. We would be failing in our duties, if we do not express our deep sense of gratitude to Prof. K. N. Shedge, Head Computer Engineering Department for permitting us to avail the facility and constant encouragement. We would also like to thank Prof. D. S. Thosar Project Co-ordinator for his great support and excellent guidance. We express our heartiest thanks to our known and unknown well-wishers for their unreserved cooperation, encouragement and suggestions during the course of this project report. Last but not the least, we would like to thanks to all our teachers, and all our friends who helped us with the ever daunting task of gathering information for the project

## REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal, ‘‘Wireless sensor network survey,’’

[2] M. Jacobsson and C. Orfanidis, ‘‘Using software-defined networking principles for wireless sensor networks,’’ in Proc. 11th Swedish Nat. Comput. Netw. Workshop, Karlstad, Sweden, May 2015.

[3] J. Qadir and O. Hasan, ‘‘Applying formal methods to networking: Theory, techniques, and applications,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 1, pp. 256–291, 1st Quart., 2015.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ‘‘Wireless sensor networks: A survey,’’ Comput. Netw., vol. 38, no. 4, pp. 393–422,Mar. 2002.

[5] I.F. Akyildiz, T. Melodia, and K.R. Chowdhury, “A Survey on wireless multimedia sensor networks,” Computer Networks (Elsevier) J., vol. 51, pp. 921- 960, 2007.

[6] J. Feng, F. Koushanfar, M. Potkonjak,"System-Architectures for Sensor Networks Issues, Alternatives, and Directions", IEEE InternationalConf on Computer Design (ICCD), Germany, 2002. pp. 226- 231.

[7] Open Networking Foundation, “Software-defined networking: the new norm for networks,” white paper, Apr. 2012.

[8] D. Kreutz, F. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76,Jan 2015.

[9] S. Scott-Hayward, G. O’Callaghan, and S. Sezer, “SDN Security: A Survey,” in Future Networks and Services (SDN4FNS), 2013 IEEE SDN for, Nov 2013, pp. 1–7.

[10] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, ‘‘Wireless sensor network virtualization: A survey,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 553–576, 1st Quart., 2016.