Software defined wireless sensor networks application opportunities for efficient network management: A survey☆

Kgotlaetsile Mathews Modieginyane[a], Babedi Betty Letswamotse[a],
Reza Malekian[a,*], Adnan M. Abu-Mahfouz[b]

[a] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa
[b] Council for Scientific and Industrial Research, Meraka Institute, South Africa

ARTICLE INFO

ABSTRACT

Wireless Sensor Networks (WSNs) are commonly used information technologies of modern networking and computing platforms. Today's network computing applications are faced with a high demand of powerful network functionalities. Functional network reach is central to customer satisfaction such as in mobile networks and cloud computing environments. However, efficient management of WSNs remains a challenge, due to problems supplemental 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 strategy for Software Defined Wireless Sensor Network (SDWSN) as an effort for application improvement in monitored environments.

1. Introduction

WSNs are sensor network technologies which are widely deployed on environmental monitoring, atmospheric monitoring, 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, cooperatively 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

---

currently pointed out as being faced by both the SDN and SDWSN approaches, in question of whether they could improve general WSN applications. We also advice on network critical aspects such as security, reliability and scalability, since these are some of the most core features that needs to be carefully considered when planning to improve or optimize network functionalities.

This paper also reflects on issues surrounding the adoption of the SDN technology in general industry networks. Our inference towards these issues comes in the form of concerns and questions that needs to be looked at with careful considerations. In these concerns, we interrogate the SDN approach applied in WSNs as to whether this technology will introduce flexibility, improve the management as well as the overall performance of WSNs. We therefore point out that, through careful considerations of the advices provided by this survey, an enormous improvement in WSN technologies can be achieved.

The rest of the paper is divided as follows: Section 2 discusses WSNs use cases, Section 3 discusses WSN protocols and topologies; Section 4 discusses WSNs, their applications and limitations. Section 5 considers SDN and its improvement positions, the advancements of SDN into mobile and wireless networks, Section 6 discusses SDN standard protocol and security aspects. Section 7 introduces SDWSN, its related work, challenges and considerations regarding its adoption. Section 8 discusses future work. Finally, Section 9 provides concluding remarks of the survey.

2. WSN case studies

2.1. 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.

2.2. 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.

3. WSNs routing protocols and network topologies

3.1. 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 overhead within the network. One critical functionality of this protocol is to utilize routing tables to store routing information.
- *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.

3.2. 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.