Ph.D. Forum Abstract: Increasing Robustness in WSN using Software Defined Network Architecture

Charalampos Orfanidis
Uppsala University, Sweden
charalampos.orfanidis@it.uu.se

***Abstract*—With the advent of Internet of Things (IoT) Wireless Sensor Networks (WSN) seem to play key a role in the connectivity of smart objects. The limited resources of WSN devices and the increased demand for new and more sophisticated services call for new and more efficient architectures. The new architectures should ensure energy-efficiency, flexibility, reliability and robustness. We believe that using SDN principles in WSN will improve many important features, such as routing, robustness and reconfiguration of the networking as well as the applications. In this research, We will find ways to increase the robustness of WSN using an SDN inspired architecture and a statistical model. The initial plan is to use statistical machine learning to look for periodic interference and other periodic behaviour in typical WSN networks.**

I. Introduction

Wireless Sensor Networks (WSN) has already arrived and is promising a whole new spectrum of services and functions. The Internet of Things (IoT) concept, which says that smart objects are able to collect and exchange data, creates new opportunities on what can be offered from ICT industry. Moreover, it outlines the necessity for new communication architectures which will enable better performance and introducing new features.

Software Defined Networking (SDN) is a new pioneering architecture for computer networking. The basic principle in SDN is that the network is divided in two planes. The *control plane*, which decides about the traffic routes and the *data plane*, which forwards the traffic packets. SDN was designed for wired networking, thus making use of it in WSN is more difficult due to limited resources and the use of wireless communication.

There have been some efforts to tailor the SDN architecture to WSN. Luo et al. in [1], designed an SDN architecture for WSN that handles packets according to a flow table. This table contains rules in the form of flow entries and the packets contain more fields than destination, source and payload. Every node when it receives a packet makes a comparison between various packet fields and the flow entries. After the comparison, an action takes place which is decided according the flow entry, such as be dropping the packet. The objective here is to add flexibility in policy changes and make it easier to manage the network. This architecture apply the basic principle of SDN, distinguish the control plane from the data plane. The data plane includes the sensors, which are forwarding the packets and the control plane consists of one (or more) controllers that functions as the brain of the network, offering routing services and Quality of Service (QoS). There are more similar attempts like [2], [3] and we expect to see more in the future.

Robustness is a system characteristic which ensures that the system will perform as expected even if the design details and the environmental conditions are unstable. In order to offer such a characteristic, first we need to determine which factors affect our system, then to what degree and finally implement a system that can function under these conditions.

A major issue for robustness is interference from external systems. As stated by Ericsson, by 2020 there will be more than 50 billion devices connected to the market [4]. According to these predictions we believe that the wireless communication interference is inevitable [5], [6]. That is a motivation for investigating a new way of increasing robustness when the presence of wireless interference is increased. Applications which are prone to interference, such as the ones used in smart buildings and operating in an environment with many other devices, would benefit from having more robust communication.

Statistical machine learning is a very effective way to recognize patterns and is used in different disciplines. In this research, we are planning to use a statistical machine learning model to identify interference patterns over time. With this, we may have an insight about interference that potentially will prevent correct networking.

The purpose of this research is to check if the proposed architecture in collaboration with a statistical model can increase the robustness in WSN. Venkatraman et al. in [7] propose an approach which detects and avoids interference, it would be interesting to compare this approach with the one we are going to implement.

II. Approach

The approach we are going to follow is based on the network architecture and the statistical model. The architecture should be designed to be energy-efficient, reliable, robust and follow SDN principles. The statistical model will be implemented in the controller which is assumed to run on a gateway node. In this way, complex computations can take place there without considering any resource limitations.

The architecture is illustrated in figure 1. The sensor nodes are operating as the *data plane*, meaning that they are able to do lightweight computations, forward data packets and communicate with the SDN controller or the *controller plane*. The SDN controller is a node with more or infinite power and

978-1-5090-0802-5/16/$31.00 ©2016 IEEE

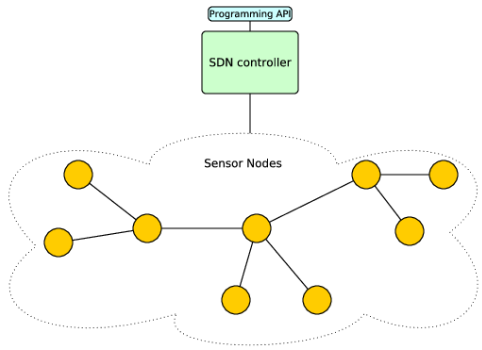

Fig. 1. SDN Architecture for WSN

more computational resources than other sensor nodes. This node is responsible of collecting the required information for the statistical model. This entity can take instructions from an administrator through an offered programming API. The SDN controller acts as the brain of the network.

The statistical model at the SDN controller may be a multivariate linear regression algorithm. This algorithm have the property of using training data and making predictions regarding a new given input. More specifically, we are planning to use as training data various characteristics of a WSN related to interference during several weeks and according to these, attempt to predict the presence of periods of high interference. Depending on the predictions, the SDN controller is responsible for doing network modifications to keep the system stable over both periods of high and low interference. Possible network modifications may be changing the using channel or the routing table. Here we can take advantage of the offering flexibility at a high level from SDN architecture, for applying the network modifications. According to these principles, we believe that the proposed approach will be able to predict and prevent network malfunctions in an efficient way.

III. Experimental Design

The first step for evaluating our approach is to do a number of simulations with Cooja [8]. Using a simulator provides the flexibility of modifying an experiment quickly and run it in a large scale. Cooja is a simulator specifically designed for WSN which is included in the Contiki [9] OS. This is also the OS we are going to use for the sensors, but we plan to do a number of modifications in order to meet the approach requirements. In this way, we will be able to confirm our initial ideas and proceed to the next step which is running experiments with sensor nodes. Observing how our approach performs in sensor nodes will give us a good insight. For these experiments we plan to use a tesbed which is deployed in Uppsala University campus building. The network coexists with university's IEEE 802.11g network. WiFi networks and Bluetooth are typically heavily used during regular working hours by students who have lectures in the same building. This would be an challenging scenario for investigating how efficiently robustness is offered, under varying levels of interference. Some parameters we are going to measure and use in our statistical model are the following:

- PDR (Packer Delivery Ratio)
- RSSI (Received Signal Strength Indicator)
- End-to-end delay
- Energy consumption
- Interference and noise

The above data or a combinations of them will be the training data for the statistical model. This would help us recognize some patterns regarding the interference which will be used to reconfigure the network in order to achieve a high level of robustness. At the same time we have to consider the limited resources of WSN to have a successful result with low overhead, something that makes the design procedure more challenging.

IV. About me

I am a first year Ph.D. student at the communication research (CoRe) group at Uppsala University. My research interests are the communication protocols for WSN and SDN. I am investigating how an SDN architecture for IoT can improve or introduce new features. I have already been involved in a research paper describing an SDN architecture for WSN which was published in a domestic workshop [10]. Before my PhD studies, I obtained a M.Sc. in Computer Science and Engineering for the Technical University of Denmark and a B.Sc. in Industrial Informatics for the Technological Educational Institute of Eastern Macedonia and Thrace. The expected time until my graduation is around 4 years.

References

[1] T. Luo, H.-P. Tan, and T. Quek, "Sensor openflow: Enabling software-defined wireless sensor networks," *Communications Letters, IEEE*, November 2012.

[2] D. Zeng, T. Miyazaki, S. Guo, T. Tsukahara, J. Kitamichi, and T. Hayashi, "Evolution of software-defined sensor networks," in *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE*.

[3] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the internet-of-things," in *NOMS), 2014 IEEE*.

[4] L. Ericsson, "More than 50 Billion Connected Devices," no. February, 2011.

[5] A. Sikora and V. Groza, "Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band," in *IMTC 2005. Proceedings of the IEEE*, May 2005.

[6] T. Boano, Carlo Albertoand Voigt, N. Tsiftes, L. Mottola, K. Römer, and M. A. Zúñiga, "Making sensornet mac protocols robust against interference," in *Wireless Sensor Networks: 7th European Conference, EWSN 2010, Coimbra, Portugal. Proceedings*, 2010.

[7] V. Iyer, F. Hermans, and T. Voigt, "Detecting and avoiding multiple sources of interference in the 2.4 ghz spectrum," in *Wireless Sensor Networks*. Springer, 2015, pp. 35–51.

[8] F. sterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja." in *LCN*. IEEE, 2006.

[9] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*. IEEE, 2004.

[10] M. Jacobsson and C. Orfanidis, "Using software-defined networking principles for wireless sensor networks," in *11th (SNCNW), 2015, Sweden*, 2015.