Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 680 – 684

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

Developing a distributed software defined networking testbed for IoT

Olivier Flauzac, Carlos Gonzalez, Florent Nolot

University of Reims Champagne-Ardenne, Laboratory CReSTIC, 51100 Reims, France

Abstract

The rapid proliferation of the Internet of Things (IoT) has led to growth in the ad-hoc networking scenario. With the recent upcoming technologies of network programmability like SDN may be effectively integrated to create a communication platform. In this work, we present the details of our preliminary study of how to determine the effectiveness of an approach to build a cluster network using Software-Defined Networking (SDN). We will provide an overview of optimum path routing protocol with cluster interaction. Our proposed scheme is a starting point for some experiments providing perspective over SDN deployment in a cluster environment for IoT. With this aim in mind, we propose a routing protocol that manages routing tasks over Cluster-SDN. By using network virtualization and OpenFlow technologies to generate virtual nodes, we simulate a prototype system controlled by SDN. Our designed testbed, is a real openflow protocol evaluation environment comprising networks and applications, which provide flexible control of framework support for large scale experiments.

Peer-review under responsibility of the Conference Program Chairs

Keywords: IoT, Software Defined Networking, Ad-Hoc networks, Cluster

1. Introduction

Today's network technology allows things and hence users, to be connected at any time at any place. With the increasing development of the internet, security threats constantly appear and the protection of data transmission has become an issue to be solved. Currently, there are more objects connected to the internet than humans in the world[1], and these generate an enormous amount of traffic (i.e., voice, video, data, etc.). All of these factors increase considerably the cost pressure on network operators, due to the emerging mobile devices and applications[2]. One of the greatest challenges concerns the security of the Internet of Things (IoT) , since it will include every object or device able to connect to wireless or wired networks[3].

In this article, we present a model to control and secure information exchanges for the IoT, based on the SDN architectures[4,5]. Firstly, the proposed model was designed to establish and secure both ad-hoc and IoT networks, in

* Corresponding author. Tel.: (+33) 3 26 91 32 15 ; fax: (+33) 3 26 91 33 97.
E-mail address: olivier.flauzac@univ-reims.fr, carlos.gonzalez-santamaria@etudiant.univ-reims.fr, florent.nolot@univ-reims.fr

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.151

order to include objects such as: sensors, tablets, smartphone, etc. Secondly, we extended the proposed architecture, and explain how flows can be routed between controllers. We demonstrate the implementation of our prototype system and evaluation results. The major contributions of this paper are:

- our work is a novel exploration of the SDN architecture to optimize the interconnection of ad-hoc and IoT applications.
- we introduce the concept of the SDN Clustered Head (SDNCH) to distribute routing functions and security rules to each edge controller.
- we introduce an implementation model with an Opendaylight controller to manage and monitor traffic from the end-users in IoT environments.

Our model is discussed later in this article, and we conclude with an outline of our vision for the SDN based solutions for ad-hoc and IoT networks.

2. SDN Cluster architecture for IoT and Ad-Hoc Network

Previously, we have proposed a Software Defined Clustered Sensor Networks (SDCSN)[10]. Clustering consists in organizing the network into groups of nodes following a hierarchical structure. Each cluster is managed by a cluster head. To develop this architecture we place the SDN controller in the cluster head. Different clustering solutions have been proposed in the literature. Some solutions propose building 1-hop clusters[14,15,17]. In those solutions, each node is at a most a distance of 1 from the cluster head, and the maximum diameter of each cluster is 2. Other solutions build k-hop clusters[18,19,20]. In k-hop cluster solutions, each node can be located at a distance at most of k from the cluster head and the maximum diameter of clusters is 2k.

Based on the approach of Model-driven Service Abstraction Layer (MD-SAL) Clustering solution active/active mode, we propose Multiple SDN Controller architecture for IoT and Ad-Hoc Networks[16]. An SDN-based architecture involves: (i) legacy interfaces (the physical layer); (ii) the SDN-compatible virtual switch (programmable layer); (iii) the SDN controller operating systems and their applications (OS layer). Ad-Hoc users will connect with other nodes through their embedded SDN-compatible switch.

Normally, a large network can not operate efficiently without some organized structure. For this reason, we propose to cluster the network and assume that each cluster head is a controller. A node state[7,8,20] can be : Simple Node (SN), Gateway Node (GN) or Cluster Head (CH). In our approach, Cluster Heads (CH) in SDCSN architecture are called SDN Cluster Heads (SDNCH). Each cluster is called an SDN Domain which is defined by :

- SDNCH is the coordinator of the domain.
- Gateway is a bridge node between Sensor Nodes and SDNCH.
- Sensor Nodes are groups of nodes in a domain together with their gateway nodes.

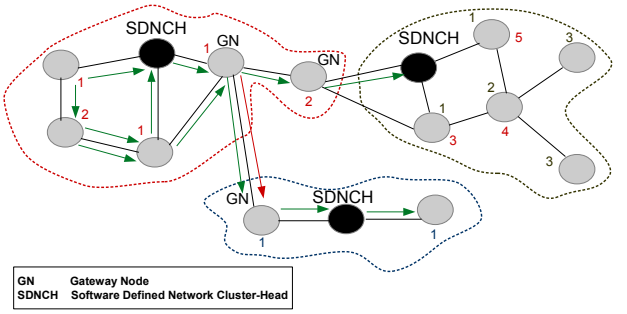

Fig. 1. Data Communication Software-defined wireless sensor networks