SDN-Based Data Transfer Security for Internet of Things

Yanbing Liu, Yao Kuang, Yunpeng Xiao, and Guangxia Xu

***Abstract*—The exponential growth of devices connected to the network has resulted in the development of new Internet of Things (IoT) applications and online services, which may have diverse and dynamic requirements on received quality. Although, the emerging software-defined networking (SDN) approach can be leveraged for the IoT environment, to dynamically achieve differentiated quality levels for different IoT tasks in very heterogeneous wireless networking scenarios, the open interfaces in SDN introduces new network attacks, which may make SDN-based IoT malfunctioned. The challenges lies in securely using SDN for IoT systems. To address this challenge, we design a SDN-based data transfer security model middlebox-guard (M-G). M-G aims at reducing network latency, and properly manage dataflow to ensure the network run safely. First, according to different security policies, middleboxes related to the defined secure policies, are placed at the most appropriate locations, using dataflow abstraction and a heuristic algorithm. Next, to avoid any middlebox becoming a hotspot, an offline integer linear program (ILP) pruning algorithm is proposed in M-G, to tackle switch volume constraints. In addition, an online linear program (LP) formulation is come up to handle load balance. Finally, secure mechanisms are proposed to handle different attacks. And network routing is solved flexibly, through dataflow management protocol, which are formulated via combining tunnels and tags. Experimental results demonstrate that this model can improve security performance and manage dataflow effectively in SDN-based IoT system.**

***Index Terms*—Dataflow management, Internet of Things (IoT), middlebox, security, software-defined networking (SDN).**

I. Introduction

THE CONTINUED evolution of new services and the growth of the information circulating the Internet, has led to the origin of ideas, concepts, and paradigms such as the Internet of Things (IoT) [1]. However, traditional network infrastructure, which need high-level network policies and configuring protocols, are inefficient and have significant limitations to support the high level of scalability and high amount of traffic and mobility. Software-defined networking (SDN) [2] decouples the traditional closed network into data plane, control plane and application plane, which enables logically centralized control and management of the whole network. With this new design principle, the network could behave more flexibly and can easily adapt to the needs of different organizations. Besides, the centralized architecture allows important information to be collected from the network and in turn used to improve and adapt their policies dynamically. Thus, as shown in Fig. 1, a programmable, flexible, and flow-centric SDN-based IoT architecture is favorable. Although, open interfaces in SDN have simplified the design of secure applications in large and complex IoT, they are vulnerable to new network attacks [3], [4], and this vulnerability inevitably reduces security in SDN-based IoT architecture. In IoT, the dataflow has to go through several processes before all required tasks are finished. Thus, proper handling of data flows in each device, is important for stable and secure network operation. Recent studies about the use of middleboxes and SDN [5]–[9] fall into three categories, including software realized middlebox, service chaining problems, and integrating traditional middlebox into SDN networks.

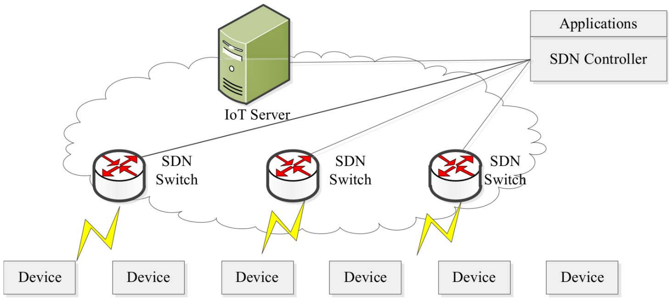

Fig. 1. SDN-based IoT architecture.

The first challenge is the dynamic of dataflow in IoT. The number of users and dataflow volume in IoT vary over time. However, most existing dataflow control techniques assume a stable network. Therefore, such techniques cannot actively consider network security. If a large number of data streams arrive simultaneously, the entire IoT network may become paralyzed. Thus, when developing dataflow control

Manuscript received August 29, 2017; revised October 16, 2017 and November 15, 2017; accepted November 24, 2017. Date of publication December 4, 2017; date of current version February 9, 2018. This work was supported in part by the National Science Foundation of China under Grant 61772098 and Grant 61772099, in part by the Chongqing Innovative Team Fund for College Development Project under Grant KJTD201310, in part by the Chongqing Youth Innovative Talent Project under Grant cstc2013kjrc-qnrc40004, in part by the Science and Technology Research Program of the Chongqing Municipal Education Committee under Grant KJ1500425, in part by the WenFeng and Foundation of CQUPT under Grant WF201403, and in part by the Chongqing Graduate Research and Innovation Project under Grant CYS14146. *(Corresponding author: Yanbing Liu.)*

Y. Liu, Y. Kuang, and Y. Xiao are with the Chongqing Engineering Laboratory of Internet and Information Security, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: liuyb@cqupt.edu.cn; 13618340827@163.com; xiaoyp@cqupt.edu.cn).

G. Xu is with the School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: xugx@cqupt.edu.cn).

Digital Object Identifier 10.1109/JIOT.2017.2779180