Secure and Flexible Internet of Things using Software Defined Networking

Stefan Mehner
Brandenburg University of Technology Cottbus-Senftenberg, Germany
Computer Networks and Communication Systems Group
03046 Cottbus
Email: stefan.mehner@b-tu.de

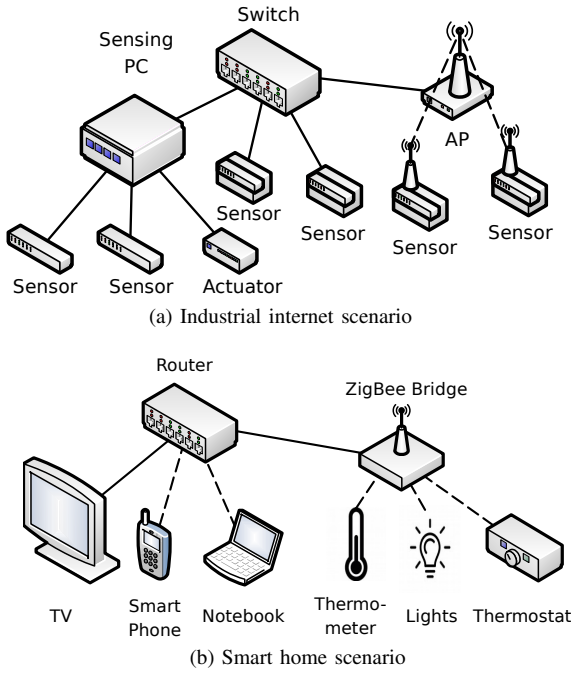
***Abstract*—There are manifold application scenarios for the Internet of Things (IoT) concept for sensing and actuation of the physical world e.g., environmental monitoring, industrial internet, smart home or healthcare. In all these use cases there are similar challenges regarding interoperability, integration and management of the devices and networks. Currently available solutions only meet individual challenges, but not all of them. The PhD thesis will tackle these challenges by using network virtualization with Software Defined Networking (SDN).**

I. Motivation

Internet connected devices are used in a vast amount in use cases like healthcare, smart home, ambient assisted living, environmental monitoring or industrial internet for sensing and actuation. There are always similar challenges regarding the integration of heterogeneous devices, their interoperability, or how to manage and configure them. Furthermore, it must be considered how to update the already deployed devices not only with new features in mind, but also for the enhancement of security in order to prevent attacks like in recent time.

To overcome the first two challenges one possible solution is the integration of the devices at the application layer. Guinard et al. [1] extend the idea of IoT to the Web of Things by implementing a web server in the devices and provide a RESTful [2] interface with well-defined semantics using the Constrained Application Protocol (CoAP) [3] over UDP. Kirsche et al.[4] follow a similar approach, but XMPP [5] with 6LoWPAN [6] is used here. The main disadvantage of this solutions is that the devices have to implement the whole TCP/IP protocol stack. This can be a bottleneck because of the high overhead, on the one hand, and the computing power and memory of the devices, on the other hand.

Another approach is network virtualization. Virtualization is a well-established concept for the abstraction of physical computing resources into logical units to allow the usage of independent users [7]. In the wired domain a paradigm, called Software Defined Networking (SDN), is tackling this idea [8]. The main idea behind SDN is to separate the control from the data plane. In other words, the packet forwarding logic is moved from switches to a centralized controller that now has a global view over the whole network. The most popular protocol for the communication between the switches and the controller is OpenFlow [9]. In OpenFlow network packets are handled in a so-called flow table. Each entry in this table describes a flow and is composed by three parts: the matching rule, the action and the statistical information. If an incoming packet cannot be associated to a flow the switch forwards it to the controller which decides how to handle this packet. This allows the configuration and the management of the whole network at one central location. New protocols, services, or policies can be introduced in a simple way. Currently research is going on to extend the SDN concepts into the wireless sensor networks domain either by adapting the OpenFlow protocol to the requirements of low-power and low-datarate networks [10] or by implementing an own optimized protocol [11].



(a) Industrial internet scenario

(b) Smart home scenario

Fig. 1. Real-world scenarios for Internet of Things applications

II. Application Scenarios

In this section we present two real-world application scenarios that suffer from the problems described. Figure 1 illustrates the scenarios.

A. Industrial Internet Scenario

The scenario in Figure 1a shows a simplified deployment of an industrial internet use case. In the current configuration sensors and actuators have either a direct wired connection or an intermediate sensing PC is used (similar to a Raspberry Pi) which has a wired connection. In the near future this scenario will be extended by wireless sensors connected with IEEE 802.15.4 as access technology. The sensing and actuation devices are used for different applications like predictive maintenance, machine status monitoring, and user information, e.g., how many units are in a packaging unit. All these devices are located in a subnet that is separated from the production network, but, as mentioned before, there are different application tasks. For this a solution is needed that enables the customer to fine-granularily separate the devices for the specific task. This is necessary because the scenario often includes different and more complicated relations between the tasks than can be represented by their physical wiring. For example the sensing devices for predictive maintenance have another owner than the other devices. Furthermore, malicious devices cannot access to all sensor data. To detect such behavior a monitoring system has to be added.

B. Smart Home Scenario

Smart home applications are a trending topic. Similar to Figure 1b, heterogeneous devices, such as TV, notebook, smart phones, light bulbs, light switches, thermostats, temperature sensors, and many more are connected wirelessly via WLAN (IEEE 802.11), ZigBee (IEEE 802.15.4), EnOcean, or other proprietary technologies. Every manufacturer provides its own bridge (illustrated as ZigBee bridge in the Figure) to the existing router of the user. Theoretically, a connection is possible at this point, but every manufacturer has its own vertical infrastructure [12] with its own data centers. In the best case, the end user can reach interoperability with services like IFTTT[1] that use high-level APIs for access to the data. Furthermore, every device in the home network can have access to all other connected devices. Recently the Mirai IoT botnet [13] showed that IoT devices can readily misused with no knowledge of the users what his/her devices are doing at the moment. For this scenario, a solution is needed that improves the security of the network without the possibility to manipulate the devices themselves. In addition, the data collection should be manageable by the owner of the data.

III. Contribution

The main research questions that will be solved using SDN are the following:

How to integrate heterogeneous things?

Most use cases deploy devices that are heterogeneous regarding memory, computing power, and communication technology. Furthermore, it can be assumed that it is not possible to manipulate the devices themselves without considerable effort. Using SDN does not require it because only the networking elements are affected. As mentioned in the motivation, it is possible to use SDN both in the wired domain as also in the wireless domain in IEEE 802.11 and IEEE 802.15.4 networks.

How to reach interoperability?

The integration of things into the Internet does not automatically enable a communication among them. With integrating different access technologies like IEEE 802.15.4 and IEEE 802.11, a protocol converter has to be used. With SDN, this can be implemented as an application on top of the controller.

How to design central management and configuration?

The controller has a global view and is able to handle the management of the network. The research focus here is how to design the central management and configuration in this heterogeneous environments with wired and wireless technologies and different network topologies.

How to improve the security of the devices?

In the concept of SDN, this use case is not designed, but SDN can improve the security of the whole network. This can be done using overlay networks, monitoring, and intrusion detection systems.

The Ph.D thesis aims developing an approach to solve these challenges.

[1] www.ifttt.com

References

[1] D. Guinard, "Towards the web of things: Web mashups for embedded devices," in *In MEM 2009 in Proceedings of WWW 2009. ACM*, 2009.

[2] R. T. Fielding, "REST: architectural styles and the design of network-based software architectures," Ph.D thesis, University of California, Irvine, 2000.

[3] C. Bormann, K. Hartke, and Z. Shelby, "The Constrained Application Protocol (CoAP)," RFC 7252, 2014.

[4] M. Kirsche and R. Klauck, "Unify to bridge gaps: Bringing xmpp into the internet of things," in *IEEE International Conference on Pervasive Computing and Communications Workshops*, 2012, pp. 455–458.

[5] P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence," RFC 6121, 2011.

[6] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*. Wiley Publishing, 2010.

[7] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: A survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 553–576, 2016.

[8] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: Taking control of the enterprise," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 1–12, 2007.

[9] The Open Networking Foundation, "OpenFlow Switch Specification," 2013.

[10] T. Luo, H. P. Tan, and T. Q. S. Quek, "Sensor openflow: Enabling software-defined wireless sensor networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1896–1899, 2012.

[11] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, "Software defined wireless networks: Unbridling sdns," in *2012 European Workshop on Software Defined Networking*, Oct 2012, pp. 1–6.

[12] Y. Li, X. Su, J. Riekki, T. Kanter, and R. Rahmani, "A sdn-based architecture for horizontal internet of things services," in *Proc. IEEE Int. Conf. Communications (ICC)*. Institute of Electrical and Electronics Engineers (IEEE), 2016, pp. 1–7.

[13] B. Krebs, "Hacked Cameras, DVRs Powered Todays Massive Internet Outage," Oct. 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/