IEEE P21451-1-5: Accessing and Managing Internet of Things Based on Customized SNMP

Jun Wu
School of Electronic Information and Electrical Engineering
Shanghai Jiao Tong University
Shanghai, China
junwuhn@sjtu.edu.cn

Wentao Zhang
School of Electronic Information and Electrical Engineering
Shanghai Jiao Tong University
Shanghai, China
zwt19971220@sjtu.edu.cn

***Abstract*—IEEE P21451-1-5 standard specifies a universal and standardized way of accessing and managing Internet of Things (IoT) based on customized Simple Network Management Protocol (SNMP). In this paper, we explain the basic concepts in IEEE P1451, provide an overview of IEEE P21451-1-5 and introduce the demonstration system to be presented in INTEROP 2020, including its building blocks, over-all architecture and the workflow of IEEE P21451-1-5 in this demonstration system.**

Introduction

IEEE P21451-1-5 standard specifies a universal and standardized way of accessing and managing Internet of Things (IoT) using Simple Network Management Protocol (SNMP), which conforms to IEEE P1451.0 standard and thus features high interoperability with other application layer protocols, such as HTTP, XMPP and MQTT.

IEEE P21451-1-5 standard, like IEEE P1451.0, is a member of IEEE P1451 standard family [1], whose goal is to define common interfaces and services for IoT, enable "plug and play" of smart transducers (i.e. sensors and actuators) and promote interoperability among transducers made by different vendors or using different protocols.

In the context of IEEE P1451, an IoT instance is carefully divided into two types of entities, named Transducer Interface Module (TIM) and Network-Capable Application Processor (NCAP), respectively. TIM is a smart transducer in which Transducer Electronic Data Sheet (TEDS) is located. TEDS is another key concept in IEEE P1451 standard, which stores comprehensive information about this transducer in a standardized format and makes the transducer self-describable, self-identifiable and therefore, "smart". NCAP is the gateway of the transducer network, who provides network services to IoT users (clients) over various application layer protocols. Such a "TIM-NCAP" division naturally results in two types of interfaces. The one between TIM and NCAP is called Transducer Independent Interface (TII) while the one between clients and NCAP is called Network Interface (NI), both of which are defined in IEEE P1451 standard.

Specifically, IEEE P21451-1-5 standard focuses on NI of IEEE P1451-compatible IoT, exploits the management functionality of SNMP and extends its usage from traditional networks to IoT, providing a universal and standardized way of accessing and managing IoT using SNMP.

Standard Overview

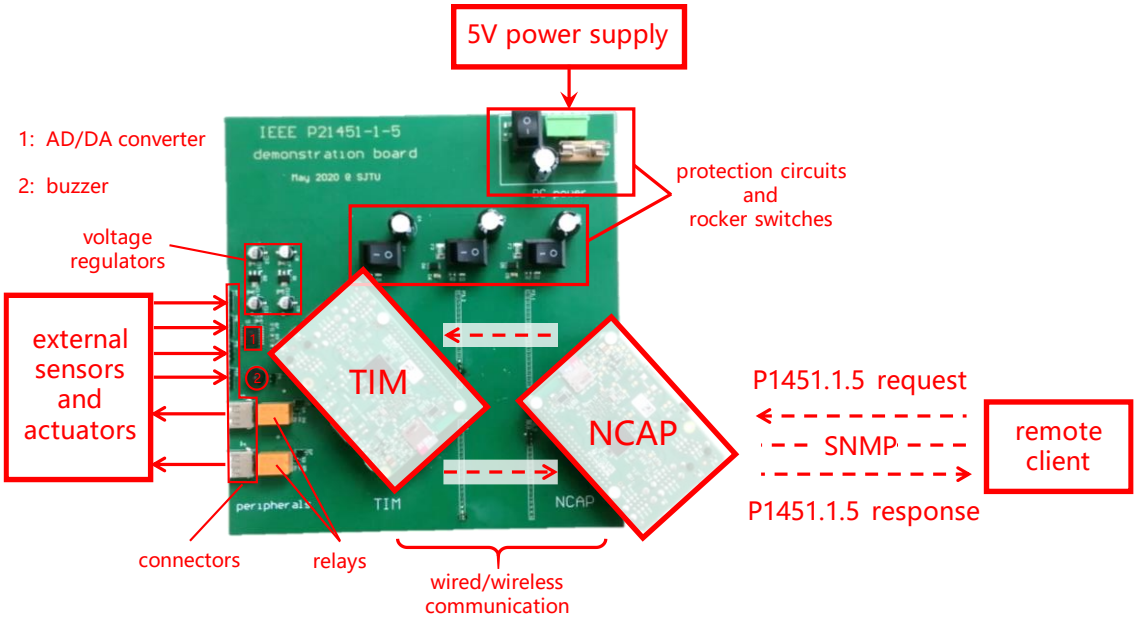
The draft of IEEE P21451-1-5 standard is under active development. This standard is aimed at addressing common issues during the process of accessing and managing IEEE P1451-compatible IoT using SNMP, and tentatively, the draft is going to include these featured contents:

- Management Information Base (MIB) tailored for IEEE P1451-compatible IoT, as well as its coordination with TEDS.
- Event notification service based on Trap PDUs of SNMP.
- Security mechanisms based on View Access Control Model (VACM) or User-based Security Model (USM).
- Time synchronization mechanism over SNMP messages.

Material and Equipment

The main components of the demonstration system are listed below:

- Raspberry Pi 3's are used as the controller of NCAP as well as the controller of TIM. On each Pi there is a Broadcom BCM2837 SoC with 4 cores and 1.2 GHz clock rate, 1 GB memory, on-board 802.11n and BLE 4.1 adaptor. Interfaces include 4 USB 2.0 ports, one HDMI port, a 100 Mbit/s Ethernet port and a 40-pin GPIO port. A 16 GB TF card is used to boot the system and also serves as the external storage. For more information about Raspberry Pi's hardware specification, please refer to the section *Useful Links and Additional Information*.
- The operating system running on NCAP is CentOS 7 for `armv7hl` architecture, while the one running on TIM is Raspberry Pi OS (32-bit), which is previously known as Raspbian and is the official operating system for Raspberry Pi.
- Various external sensors and actuators, for example, temperature sensor, photosensitive sensor, humidifier, fan, lamp and so forth.
- A specially designed motherboard connects different parts of the system. It is a printed circuit board and should be powered by an external DC power supply with 5V output. It features protection circuits against



overvoltage or short circuit, voltage regulators that generate 3.3V power supply, and rocker switches that enables the operator to control the on/off status of different subsystems. It has sockets and mechanical connectors whereby Raspberry Pi's can be reliably installed. It provides pin headers to which external sensors and actuators can be connected. On the board itself there is an AD/DA converter chip that can perform signal conversion, an alarm buzzer and several relays, which are controllable and can be considered as on-board actuators.

- A switching power supply with 5V/20A output is used to drive the whole system. Note that the power consumption of the system is much less than the supply and "5V/20A" is only chosen for redundancy and for scalability in the future.
- Keyboard, mouse and display can be connected to the system for programming, debugging and testing.

Demo Structure

Combining together all the components introduced in the last section, we obtain the demonstration system's overall architecture, as shown in the figure.

The process of accessing or managing IoT using SNMP goes as follows: Firstly, a client on the network initiates a request that is packed in P1451.1.5 format (that is, "1451.1 over SNMP") and is sent to NCAP. Secondly, NCAP receives the request message, resolves it, translates it into standardized 1451 commands that can be recognized by TIMs (that is, "calls transducer services") and then issues the commands to certain TIMs. The transmission in this step can either requires a physical cable between NCAP and TIM (using protocols like UART) or goes over the air (using Wi-Fi, BLE, etc.). Next, TIM responds to the commands by reading a sensor or regulating an actuator's output, and replies with a response message. At last, the response message goes in reverse as the request message and is sent back to the client.

Useful Links and Aditional Information

1. Project main page of IEEE P21451-1-5 standard:

   https://standards.ieee.org/project/21451-1-5.html

2. Hardware specification of Raspberry Pi 3B:

   https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

3. Popular open-source SNMP implementations:

   `net-snmp`: http://www.net-snmp.org/

   `pysnmp`: https://github.com/etingof/pysnmp

4. Some of the published research papers related to this topic are [2], [3] and [4].

Acknowledgment

The IEEE P21451-1-5 working group would like to express their very great appreciation to Kang Lee, Eugene Song and Victor Huang, for their generous help and insightful suggestions during the whole process of standard development.

References

[1] E. Y. Song and K. Lee, "Understanding IEEE 1451-Networked smart transducer interface standard - What is a smart transducer?," in IEEE Instrumentation & Measurement Magazine, vol. 11, no. 2, pp. 11-17, April 2008, doi: 10.1109/MIM.2008.4483728.

[2] Longhua Guo, Jun Wu, Jingwei Li, Jianhua Li and W. J. Miller, "A lightweight secure time synchronization mechanism for ISO/IEC/IEEE 21451 sensor networks," 2015 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), Beijing, 2015, pp. 13-18, doi: 10.1109/ISPCS.2015.7324673.

[3] X. Feng, J. Wu, J. Li and S. Wang, "Efficient Secure Access to IEEE 21451 Based Wireless IIoT Using Optimized TEDS and MIB," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, 2018, pp. 5221-5227, doi: 10.1109/IECON.2018.8591182.

[4] J. Ren, Y. Liu, J. Wu, J. Li and K. Wang, "Smart NCAP supporting Low-Rate DDoS Detection for IEEE 21451-1-5 Internet of Things," 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 2019, pp. 532-535, doi: 10.1109/ICPHYS.2019.8780132.