RIOT Summit 2018 – Report

Julien Gomez Trong-Vu Tran

Abstract—**In September took place the RIOT Summit 2018. For this occasion, we attented numerous keynotes and talked to some developers who were interested in our thesis. On the first day, we discovered other RTOS that could be benchmarked: *Apache Mynewt, Zephyr, MbedOS, Contiki-NG*. On the second day, we discovered service like *The Things Network* and *IoT-Lab*. During the conversations with the developers, many gave us some advices for our thesis. Our next step is to contact the IoT community to gather more advices and information on the benchmarking of real-time OS.**

I. INTRODUCTION

FOR our master thesis "Benchmarking of Real-Time Operating Systems for Internet of Things", we went to the RIOT Summit 2018 in Amsterdam.

This was the third summit of the RIOT community. Every year the members of this community gather and talk about their projects and the future work for RIOT-OS.

The summit was divided into two days. During the first day, 12 speakers presented their work. On the second day, tutorials were given and breakout groups ended the summit. More information can be found on the summit website.

This report will present what we learned during these two days and what will be useful for our master thesis.

II. FIRST DAY

During the first day, 12 talks were given by IoT developers and enthusiasts. For each of the keynotes, we describe what we learned and what will be useful for our thesis.

Notice that we do not mention all keynotes as some of them are irrelevant for our master thesis.

A. From R&D to production – Jaime Jiménez

In the IoT world, many standards exist. In the connectiviy layer, we can find 6LOWPAN, LORAWAN, ROLL, . . .
In the applications layer, COAP, CBOR, . . .
In the security layer, COSE, DICE, . . .

The speaker showed us that the IoT world is shared among four major "players":

- System integrators,
- Cloud providers,
- Telecom infrastructures and
- Operators.

Between these major players, there is still room for innovative startups. Jaime Jiménez showed us some examples like *Smart Rockbolt* or *IOTEROP*.

In conclusion, we learned that the IoT world is complex with a lot of standards. Many of these standards are open-source. This helps startups to immerge from a highly competitive world among big players like Google, IBM or AT&T.

Slides are available here.

B. NimBLE - Portable bluetooth stack from Apache Mynewt – Szymon Janc

The talk explained the implementation of the Bluetooth Low Energy (BLE) technology into Apache Mynewt, another RTOS. It is integrated as a module called NimBLE. A brief presentation of the Bluetooth technology and its evolutions was given. Then the presenter talked about the Apache Mynewt project. The last part was about refactoring the NimBLE module to port it into other OS's.

In conclusion, this talk was interesting as we could see how the stack was implemented and ported. It could be a good starting point if we decide to benchmark BLE.

Slides are available here.

C. Google Protocol Buffers for embedded IoT – Morgan Kita

JSON or XML formats are highly portable and human-readable but cost a lot in IoT ecosystem. Storing, parsing or sending JSON/XML files is too complex for small embedded devices. Other solutions that use binary format exist but they loose the portability and the human-readability value.

Morgan Kita showed us the pros and cons of a system using the Google Protocol Buffers. In the IoT world, *Nano-PB* implements this protocol.

What we've learned from this talk is that JSON, XML or other high-level formast can be costly for RTOS.

Slides are available here.

D. Resource discovery, Object Security and other news from CoAP – Christian Amsüss

This talk gave an introduction to the CoAP protocol and its recent and ongoing developments mainly in term of security and network topology.

The first part of the talk was about the CoRE Resource Directory, a centralized directory where servers (i.e. devices) can register their resources. Clients can then request a particular resource with a single request to the RD (i.e. Resource Directory). He then explained in more details the

aspects and advantages of this topology.

The second part of the talk was about OSCORE (Object Security for CoRE). The principle is to hide a CoAP request or response into a generic encrypted CoAP request or response. For example, a GET request for a resource is hidden into a POST request which hides the resource that the client wish to access. The POST request contains 2 special fields:

- Object-Security which is used to share a key and a nonce (depending on the encryption scheme used),
- Encrypted payload which is the actual request encrypted.

The same mechanism applies with the response.

Slides are available here.

E. Build a robot with RIOT – Gilles Doffe

For the Robotic Cup 2018, *Savoir-faire Linux* built a robot using RIOT-OS. The main part we will focus on for this keynote is the architecture and the scheduling they use for their robot. They implemented three threads: one for the motion control, one for the planner and one for the analog sensors.

The *Savoir-faire linux* team struggled with the scheduler of RIOT-OS. The RTOS provides a tickless, preemptive and priority based scheduler.

After speaking with Gilles Doffe, we understand more how the scheduler of RIOT-OS works. For our thesis, we will take into account the type of scheduler used by the benchmarked RTOS.

Slides are available here.

F. New Crypto-fundamentals in RIOT – Pieter Kietzmann

The speaker talked about the lack of secured hardware in Commercial Off-the-Shelf IoT devices such as Intel SGX or ARM TrustZone. Those devices require efficient security softwares implementations that can be contained within their constraints.

He presented what is called Physical Unclonable Functions or PUF, functions that are based of physical characteristics of a particular device (such as components delays, magnetism or some patterns in the uninitialized memory). With those kind of functions, a single device own an unique fingerprint which is different from another device (even from the same batch) due to variations in the manufacturing process.

He then explained the problematic of noise in the process of generating and authenticating a device using PUFs. After that, he presented his implementation of a SRAM based PUF using RIOT for generating PRNG seeds and keys.

What we can retain from this presentation is that implementing entropy using a constrained device (for key or seed generation for example) is not easy. Benchmarking and analyzing the current implementations

PRNG's in RTOS's could be very interesting (distribution, bias, uniqueness).

Slides are available here.

III. SECOND DAY

The second day was shorter than the first one. Two tutorials were given at the same time: one for beginners and one for the maintainers. We went to the beginner one. This tutorial comes from a RIOT course available on Github.

With this short beginner introduction to RIOT, we discovered service like *The Things Network* and *IoT-Lab*. The sooner is an interface that allows us to access the `LoraWAN` network. The later is a large infrastructure that gives access to hundreds of nodes for testing purposes.

IV. ADDITIONAL INFORMATION

By talking with the developers that were present at the summit, we learned that the STM32F4 series microcontroller is a good choice. With its ARM Cortex-M4 based MCU, it compiles a large variety of RTOS.

Additionaly, we talked about our idea to use a logical analyser. Gilles Doffe from *Savoir-faire Linux* confirmed our opinion about using this kind of devices for our benchmarking.

V. CONCLUSION

During this summit, we discovered a large number of applications of RIOT-OS. We talked to some of the maintainers of RIOT-OS and other developers. With their expertise and their advices, we get references to hardwares and softwares that could be useful for our master thesis.

What we will do next is to contact those who gave us their contact information and ask them for recommendations. We will also get in touch with the IoT community via mailing list.