Connecting Smart Objects to Wireless WANs

Suresh Krishnan
suresh.krishnan@ericsson.com

Abstract

This paper explores the possibility of connecting an extremely large number of Smart Objects directly to wireless WANs (WWANs), such as LTE, in order to vastly expand the locations at which these smart objects could be placed. It discusses the challenges that need to be addressed on the WWAN side as well as on the smart object side.

Introduction

The number of connected smart objects is expected to grow exponentially in the near future. As smart objects start getting used for more and more applications, it is highly likely that a large number of these devices will be placed in environments where WWANs are the only available method of connectivity (e.g. remote areas, inhospitable environments etc.). Unfortunately, the WWANs were not designed with these sorts of connected devices in mind. The procedures for attaching to such networks, staying connected and transmission/reception of data were geared towards much more powerful and always-on devices. This discrepancy leads to some issues for smart objects.

1. Power Usage

The WWAN networks usually provide for some form of low power operating mode ("idle mode") on the attached devices. Even in these idle modes the power usage on the device is in the order of several milliwatts (mW). With this level of power consumption battery operated devices will run out after operating for a few days. In the kind of deployments where WWAN connectivity is necessitated, it is highly impractical to replace batteries at these frequencies. Fortunately, the actual power required for transmitting over such radio interfaces is only in the order of a few microwatts (μW) thus yielding the possibility of a 1000 fold increase in battery life. This requires significant changes to the WWAN procedures but is very much doable.

2. Signaling overhead

The WWAN networks were defined with mobility and quality of service (QoS) as the most important requirements. In order to fulfil these requirements, attachment to a WWAN involves several rounds of signaling over the radio link and associated signaling over the core network in order to get anchored with a suitably located mobility anchor point within the WWAN. This signaling overhead is easily amortized over long lived

connections that are typical in always-on devices (e.g. smartphones) that transfer large volumes of data. But for the kind of applications (low bandwidth and intermittently connected) that are usually targeted by smart objects this overhead is prohibitively expensive.

3. Spectrum availability

The operators of WWAN networks have access to a limited amount of spectrum that they probably acquired at a great cost. Due to the aforementioned signaling overhead even low bandwidth transmissions from intermittently connected devices cause a lot of load on the signaling (control) channels as a radio resources have to be allocated before each transmission and be freed after each transmission. This will limit the number of smart objects that can be connected to the WWAN even though the actual bandwidth usage is miniscule. As spectrum resources are finite and limited, the current control paradigm in WWANs need to be modified if they need to scale to support billions of smart objects.

4. Identification and Configuration

With the large number of smart objects, it becomes very difficult to manually configure these devices and positively identify and manage them in the network. The configuration mechanisms need to be very lightweight without putting a significant load on the control plane of the WWAN nodes. The configuration mechanisms also need to provide unique addresses to the smart objects with a low overhead. A modified version of IPv6 stateless auto-configuration (SLAAC) may be one such mechanism that can allow the smart objects to create their own (unique) addresses.

5. Security

Many of the deployments of smart objects would require that the data received from the smart objects be tamper-proof and be subject to some form of data origin authentication. The WWANs currently provide strong security and mutual authentication but these procedures may be too heavyweight for the smart objects. More lightweight security mechanisms may be required, but this can be accomplished fairly easily by leveraging some form of shared information between the WWAN and the smart object. It is also essential that the WWAN protect itself from DDOS attacks mounted by botnets consisting of a large number of connected smart objects.

Conclusion

This paper identified some issues with the connection of smart objects to WWANs. There is some ongoing research to fix these issues. The good news is that it looks like none of these issues are insurmountable and most of them can be addressed using fairly minor changes to control and signaling procedures in WWANs.