



Future Internet PPP Architecture

Position paper No1: Connecting Internet of Things with the Current Internet

From: EIT ICT KIC/Helsinki Node
Comnet/Aalto University

Prof. Raimo Kantola, Jukka Manner
{firstname.lastname}@tkk.fi

Critical Analysis

New business opportunities in Future Internet largely make use of real world sensors and actuators owned by consumers. Further scaling up of the Internet largely takes place by connecting new consumers and new devices owned by the consumers. The rate of adoption of mobile broadband has overtaken the rate of adoption fixed broadband. Also, the number of mobile broadband subscriptions is already larger than the number of fixed broadband subscriptions. The consequence is that most devices connected to the Future Internet are battery powered. The wireless Internet will continue to grow because with the modern EDGE/WCDMA/HSPA/LTE technology it is economically feasible to build wireless broadband access today into most large cities in the emerging markets with a total population of more than 2 Billion. The economic feasibility of Mobile broadband in developed markets is also evident.

There are two significant hindrance factors to deployment of solutions involving battery powered devices. One is that there is no uniform and agreed way of making these devices reachable on the Internet using an interrupt driven architecture. The recommended solution is UNSAF that uses polling leading to fast depletion of the battery. Moreover, UNSAF requires application specific code in hosts. Other, tailor made, application level solutions are also being proposed. The second issue is that once reachable, a wireless device becomes vulnerable to attacks and unwanted traffic. The well known protection tools that work on PC's do not scale to battery powered devices. A firewall on a battery powered device will only deplete the battery faster leading to DOS. These problems apply equally well to mobile devices.

Recommendations for Advancement of Technology

We propose that generic access architecture is needed for connecting the Internet of Things with the current Internet. The architecture should support interrupt driven access of sensors, actuators and mobile devices and computers and protect those devices from unwanted traffic at the same time. To achieve the latter goal, before admitting a flow to a battery powered device, an access node should be able to establish *trust* between the sender of the flow and the targeted device. The access node should be able to follow the policy that is appropriate for the application. This means that the access node must be able to assure with a high level of confidence that the source is legitimate for the target before the node admits the flow. Overall, we call the range of mechanisms for establishing the needed level of trust *packet access control* in the access node.

The above functional requirements translate into the technical requirement of separating addressing and Identity in the protocol stack. Identity is the key to trust functions and packet access control while addresses are used for packet forwarding into the right target. Consequently, translations between the ID and the addresses must be supported by the architecture in a secure manner. Also, either the architecture assumes that there is an algorithm for producing identity from a name and consequently, the ID is just another representation of a name or the architecture provides a translation from names to IDs.



Future Internet PPP Architecture

Many battery powered devices are too small for a fully blown IP stack. Therefore, dedicated protocols are sometimes used over the wireless link. The access node, besides providing trust and reachability, should also be capable of accommodating several different forwarding protocols. The overall access architecture should accommodate mobility of devices and multi-homing of the access nodes themselves. Information transport is moving from synchronous networks to asynchronous packet networks that in practice will be based on Ethernet, including Energy Efficient Ethernet (802.3az) and others. It should be possible for the access node to forward traffic directly over Ethernet as well as over IP. The former will be first relevant in scenarios where power saving is crucial.

In the PPP we at EIT/Helsinki node (Comnet) propose to create the generic trust and reachability access technology that is needed for connecting the Internet of Things with the current Internet. The access node is called Customer Edge Switch: for controlling the flow of traffic it uses connection state allowing the deployment of sophisticated control mechanisms for validating the flow before it is admitted to the battery powered target. A component of the proposed solution is the new Trust-to-Trust Protocol (T2P) that supports several different kinds of Identities for different levels of desired confidence on the sender. In addition T2P hides the target network from the world protecting its privacy. For highest levels of trust the solution envisioned so far leverages the existing 3G mobile network infrastructure owned by the mobile operators. The architecture is open to extensions for supporting other trust mechanisms and infrastructures.

Future Orientation

The current technology uses firewalls and NATs to hide and protect the hosts and user networks from harm. These are called “middle-boxes” and are seen as violations of the “Internet architecture” that is supposed to follow the end-to-end principle. Customer Edge Switching (CES) makes the functionality of NATs and Firewalls legitimate parts of the Internet architecture, implements the principle of Trust-to-Trust and is driven by mobile and wireless use. CES is a technology that can advance the European mobile industry, leverage the mobile operator’s infrastructure and spur innovation in the area of Internet of Things.

What can EIT Helsinki Node/Comnet Contribute now?

We have developed a blueprint of the solution and done the first experiment with it. A more advanced implementation work is ongoing. We have published the definition of a new protocol called Trust-to-Trust protocol for CES to CES communication. Each party can make an independent investment decision on CES and benefit immediately. The solution interworks smoothly with legacy IP sources and destinations. We have built the competence to develop the technology till it can be moved to industrial partners.

Experimentation Facilities

It would make sense to set up a European wide experiment using the NREN facilities and the FIRE or a new similar framework created by the FI PPP.

More information on the site: www.re2ee.org.