# IPv6 at the Edge of the Cloud

Brad Campbell, Zakir Durumeric, Prabal Dutta
Electrical Engineering and Computer Science Department
University of Michigan
Ann Arbor, MI 48109
{bradjc,zakir,prabal}@umich.edu

## Abstract

When looking at the new devices and operating modes that will emerge to comprise the "swarm" of sensors, we must consider the networking layer that will connect them to the cloud and the Internet at large. IPv6 and 6LoWPAN have been proposed and studied for wireless sensor networks, but new sensor types, such as energy-harvesting, millimeter-scale, and transmit only nodes, as well as new deployment strategies for city-wide scale may require rethinking, or at least tweaking, this approach. We believe that IPv6 is still viable, and in fact quite useful, for this application. However, how to fully integrate these new devices raises some challenges for future deployments.

## 1 Introduction

Traditional, battery-powered wireless sensor networks have been shown to benefit from IPv6 [1]. These nodes maintain a low radio duty cycle but still regularly participate in the network. They have predictable wakeup times and can support the various networking protocols that IPv6 provides. Also, deployments of these traditional networks are typically small or localized to a specific area and type of node. This simplifies the network layer requirements and requires less infrastructure to connect the deployment to the Internet.

When we drive down the functionality of nodes in the network, by using energy-harvesting power supplies, scaling the nodes down to $mm^3$ sizes, or using other means to meet cost, power, and density goals, we break some assumptions of IPv6 and 6LoWPAN sensor networks. For example, energy-harvesting nodes often do not have predicable wakeup times and may effectively be transmit only nodes.

Future deployments, particularly when looking at city-scale, will consist of many different types of fixed and mobile sensors interacting in real time. Deployments may also change over time, and a particular network can't assume it will always be isolated.

While considering these types of issues here are some preliminary issues that we've encountered:

**How do we handle routing?** As IPv6 adoption is slow, and the swarm would benefit from having full IPv6 deployment, how do we bridge the gap? What techniques can we use to deploy today while planning for the future?

**Transmit only node addresses.** If a node is not equipped to receive packets, that is, it does not have a reliable wakeup time, it cannot learn its own full IPv6 address. Is this a problem? What about calculating checksums?

**How do we know where to route?** If nodes are mobile, or optimal routes between nodes change, the border router a node is using as its gateway to the cloud could change. If we would like to send packets *to* that node, how do routes adapt to this new entry point to the wireless network?

## 2 Routing to Embedded Networks

Many border routers that act as a gateway between the installed IPv6 networks and wireless sensor networks will have to exist to support large numbers of these wireless networks. These border routers must be able to advertise the prefix of the wireless network they manage or have a route for that prefix statically assigned to them. However, these border nodes are typically not managed by the same group that manages network infrastructure. These border nodes do not run typical interior gateway protocols, such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF). Regardless of whether these nodes were physically capable of running such protocols, organizations may not be willing to delegate maintenance of an enterprise routing infrastructure to embedded systems maintainers. While static routes suffice in the short term, as sensor networks become ubiquitous, maintaining static routes will become burdensome to network administrators.

## 3 Transport Layer Protocols Expect Full Addressing

Transmit only nodes can only mimic true IP nodes and fall noticeably short in one key area: they cannot learn their own address. Short of configuring them in a non-maintainable way (e.g. at compile time), transmit only nodes have no method of determining the IPv6 prefix of their network as both DHCPv6 and stateless autoconfiguration require the node to receive a packet containing the prefix. Knowing its own prefix is not strictly required to send a valid 6LoWPAN packet and through the use of *stateful* source addressing, a transmit-only node can send a 6LoWPAN packet without ever knowing its own prefix. However, defacto transport layer protocols, including both TCP and UDP, both require full knowledge of network layer addressing in order to compute a transport layer checksum.

In order to remedy this situation, border nodes must check and recalculate transport layer checksums along with expanding compressed portions of the IPv6 header before routing the packets onto the public Internet. There are sev-

eral simple solutions including an application layer checksum or for a border node to check the checksum and recalculate a new checksum for every packet. However, with border routers no longer being simply stateless and packets that require higher layer manipulation, at what point is mimicking IPv6 no longer the best option for these networks?

## 4 Routing to Nodes with Changing Addresses

While the IP addresses of conventional servers do not often change without notice, the full routable IPv6 address of a specific 6LoWPAN embedded device can change without notice due to trivial changes within the embedded network such as the addition or removal of a path critical node. If the optimal path changes such that a node uses a different border router as a gateway, the prefix of its address could likely change. This raises the immediate question over the optimal methodology for determining the the full address of and route to a specific node given that the correct border router may not be known. There are several potential solutions: (1) route packets to every border node of an embedded network, (2) advertising new addresses to a mediator, (3) all border routers advertise the same prefix. However, each of these have their own downfalls. The first places unnecessary burden on all border routers of the network, the second requires additional external infrastructure, regular route calculation and network traffic from each node, and the third requires complex routing rules that may not available to all organizations.

## 5 Conclusions

IPv6 and 6LoWPAN offer a convenient network layer for the use with a city scale swarm of sensors. However, several issues arise in practice with new, extremely limited sensor nodes. We have explored these issues and preliminary solutions, but more discussion is needed to find the correct path forward.

## 6 References

[1] J. W. Hui and D. E. Culler. Ip is dead, long live ip for wireless sensor networks. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, SenSys '08, pages 15–28, New York, NY, USA, 2008. ACM.