IPv6 WSN Geolocation Using the MAC Address

T O’Daniel
Asia Pacific University of Technology & Innovation
dr.thomas.odaniel@apu.edu.my

Abstract. Wide-area Wireless Sensor Network (WSN) deployments that consist of a large number of distributed nodes can benefit greatly from self-configuration and constant reporting of the location where data was sensed. Previous work has shown how a WSN node can calculate an initial estimate of its location and a finite set of alternate points that could be its actual location, using the coordinates and nominal transmission radius of its neighbours embedded in their IPv6 addresses. This paper extends that work, presenting a scheme for embedding the coordinates in the Ethernet MAC address to allow use of IPv6 header compression. To save energy, a practical and efficient method for exchanging neighbor address information and supporting dynamic address changes is also proposed to replace listening in promiscuous mode. Necessary modifications to the stack are identified, and a test program is outlined.

1. Introduction

Wireless Sensor Networks (WSNs) are a fundamental aspect of ubiquitous systems and the Internet of Things (IoT). WSNs are composed of low cost tiny devices with constrained processing and memory resources that are typically battery powered. Networks of these devices are characterized by small packet payload size, minimum bandwidth, unreliable radio connectivity, ad hoc deployment, and nodes running in a power conservation mode to prolong battery lifetime. Many types of WSN deployments, particularly for environmental surveillance and disaster management could benefit from constant reporting of the location where data was sensed. Nodes can be equipped with Global Positioning System (GPS), but this is costly in terms of both money and energy consumption.

Previous work [1] has shown how a WSN node in a network that has a small number of sparsely distributed nodes with GPS ground-truth can calculate an initial estimate of its location and a finite set of alternate points that could be its actual location, given the coordinates and transmission radius of two or three neighbors. The technique presented there embeds the GPS coordinates and the nominal transmission radius for a node into its IPv6 address, so the necessary information can be acquired by passively listening to transmissions. As with all WSN localization techniques, a primary goal is to derive a satisfactory degree of accuracy from inconsistent radio communication while minimizing power consumption; further design goals are Internet standards compliance and minimal modifications to standard implementations.

This paper extends that previous work in two directions. First, the global location coordinates and the nominal transmission radius for a node are embedded in the Ethernet Media Access Control (MAC) address to facilitate the use of IPv6 header compression. Second a practical and efficient method for exchanging neighbor address information and supporting dynamic address changes is proposed, to replace listening in promiscuous mode.
The next section provides basic background on how the previous work used global position coordinates in the network addressing scheme. This is followed by a description of the initialization process for an IPv6 over Ethernet network, and the 6LOWPAN adaptation layer. Section 4 describes the scheme for encoding the coordinates, required preconfiguration, the process of distributing location information, and a method for supporting MAC address changes when a node refines the accuracy of its position location estimate. The final section summarizes the modifications that need to be made and outlines the test program.

2. Background

The IPv6 network is designed to work optimally with efficient links and high packet delivery rates, which is quite the opposite of the general characteristics of WSNs. These low-power and lossy networks do not typically have predefined topologies, for example, those imposed by point-to-point wires, so “on-link” simply means within radio range, protocols must tolerate sleep cycles where the node will not transmit or receive, and small packet sizes limit throughput.

The IETF standard for extending the use of IPv6 to WSNs is known as 6LoWPAN, which stands for “IPv6 over Low Power Wireless Personal Area Networks”. A typical protocol stack has standard Internet protocols at the transport and application layers, IPv6 at the network layer, a 6LoWPAN adaptation layer, and IEEE 802.15.4 at the data link and physical layers.

IEEE 802.15.4 was developed for interconnection of data communication devices using short-range radio frequency (RF) transmissions in a wireless personal area network [2]. This standard defines a maximum physical-layer packet size of 127 octets, while IPv6 at the network layer requires support for a Maximum Transmission Unit (MTU) of at least 1280 octets over the link. Furthermore, the physical and Media Access Control (MAC) layer frame overhead can be up to 25 octets, which with the IPv6 header of 40 octets leaves only 62 octets for link-layer security and upper-layer protocols. The 6LoWPAN adaptation layer provides header compression along with packet fragmentation and reassembly mechanisms to manage these differences transparently.

2.1. Addressing

MAC addresses are formed according to the EUI-48 name space managed by the IEEE: EUI is an acronym for Extended Unique Identifier [3]. The leftmost 24 bits is a ‘prefix’ registered to the adapter manufacturer, and the remaining 24 bits are an identification number for the specific device. The first octet of the address has two reserved bits: the U/L bit, short for Universal/Local, which identifies how the address is administered, and one bit to flag a group address. Packets sent to a group address are accepted by all stations on a LAN that have been configured to receive them. Packets sent to the broadcast MAC address, all one bits, are forwarded to and accepted by all nodes.

The IPv6 addressing architecture [4] defines the general unicast address format as an 8 bit prefix to identify the address class, a 40 bit Global ID allocated by the Internet service provider; a 16 bit Subnet ID determined by the site; and a 64 bit Interface ID (IID). The IID needs to be unique on the links reached by routing to that prefix, so the full IPv6 address is unique within the applicable scope. There are no broadcast addresses in IPv6, several multicast addresses are used instead.

Every node on the network is also required to set and recognize a Link-Local address for each interface, and a Solicited-Node multicast address for the other addresses configured for each interface. The Link Local IPv6 address is formed using a predefined 8 bit prefix 0xFE80, setting the 40 bit Global ID and 16 bit Subnet ID to zero, and (typically) using the MAC address in Modified EUI-64 format as the 64 bit Interface ID. A Solicited-Node multicast address is formed by appending the lower-order 24 bits of an address to a defined 104 bit prefix. This is designed to reduce the number of multicast addresses a node must join.

Unique Local IPv6 Unicast Addresses, intended for communications inside a site [5], have prefix 0xFD00 and set the 40 bit Global ID to a pseudo-random number using a standard algorithm. The IPv6 addressing architecture originally required the IID to be constructed in Modified EUI-64 format, meaning hexadecimal value 0xFFFE is inserted between the company ID and vendor supplied ID of
the IEEE 48 bit MAC identifier, and the U/L bit is inverted. In 2014 this restriction was removed, so the bits in an interface identifier have no generic semantics and for the purposes of IP, the entire identifier is treated as an opaque value [6].

2.2. Global Positioning Coordinates
The World Geodetic System of 1984 (WGS84) is the global reference system for geospatial information, and the reference system for the Global Positioning System (GPS) [7]. Location coordinates are based on dividing the ellipsoid of the earth into 360 degrees of horizontal longitude and 180 degrees of vertical latitude. Zero degrees longitude is an arbitrary line, with locations to the west given negative numbers while locations to the east are positive, for an overall range of -180 to +180. Zero degrees latitude is the equator, with locations to the north as a positive number and to the south as a negative number, for an overall range of -90 to +90. Each degree of latitude and longitude is divided into sixty minutes, and each minute is divided into sixty seconds. Three common formats for this are ddd°mm's'ss", ddd°mm.mmm', and ddd.ddddd°.

At the equator, one degree of latitude or longitude represents approximately 111 km and a minute is approximately 1.85 meters. Because the meridians get closer together moving from the equator toward either pole, the physical distance represented by degree of longitude gets smaller. At 45 degrees north or south latitude (Portland OR USA; Limoges, France; Harbin, China // Rio Mayo, Argentina; Dunedin, New Zealand) the fourth decimal place of dd.ddddd° represents approximately 7.9 meters and the fifth 79 cm. The fourth decimal place is also the typical accuracy of an uncorrected GPS unit with no interference, and accuracy to the fifth decimal place can be achieved with multiple readings from several commercial GPS units. The seventh decimal place is near the limit of what GPS-based techniques can achieve with painstaking ground-truth measurements [7].

2.3. Location Interpolation
Wireless networks are inherently broadcast, so every node within range of a given node can hear all transmissions. The previous work [1] shows how location coordinates embedded in the source and destination IPv6 address allow a node to acquire the location of every neighbor by passively listening to transmissions. Once a list of neighbors has been assembled, a library of efficient functions is used by the listening node to estimate its location as the farthest point from which it can maintain communication with its neighbors, along with a finite set of (closer) alternative locations. The base cases work with minimal information, presuming a network begins with a small number of nodes transmitting their pre-configured address. Other nodes discover these as neighbors, locate themselves, and begin transmitting, providing the next layer of listening nodes with the information required to locate themselves, and in turn providing new point of reference that other nodes can use to refine their position estimate within the bounds of their set of alternative locations.

Section 4 describes how this method is used with the global location coordinates embedded MAC address, along with a practical and efficient method for exchanging neighbor address information and supporting dynamic address changes to replace listening in promiscuous mode after the network initialization phase.

3. Environment
Before manipulating the MAC address it is important to know how it is used, and to evaluate the viability of the assumption that neighbor can be acquired by passively listening to transmissions, it is important to know the messages exchanged during network initialization.

3.1. IEEE 802.15.4 Operating Modes
There are three operating modes defined by IEEE 802.15.4: PAN coordinator, coordinator, and end device. Each network has exactly one PAN coordinator, providing synchronization services to other devices and coordinators. The bulk of the standard is devoted to the behavior of beacon enabled
networks, which assume a mains-powered PAN coordinator will be common; ZigBee and Bluetooth LE rely more heavily on these facilities.

For PANs not supporting beacons, synchronization may be done by polling the coordinator for data, which leads naturally to a star topology. A peer-to-peer topology still has a single PAN coordinator and operates in beaconless mode, but any device can communicate with any other device in range. The standard mentions the cluster tree as a special case of a peer-to-peer network, where the PAN coordinator forms the first cluster and may instruct another device to act as a local coordinator to form a new cluster adjacent to the first one. Local coordinators may in turn designate other local coordinators to form additional clusters to meet coverage requirements.

3.2. IEEE 802.15.4 Network Initialization
IEEE 802.15.4 requires every node to perform a scan of available radio channels before joining a PAN, and every node to join a PAN before sending data frames. The standard defines four types of scan: Active, Passive, Energy Detect (ED), and Orphan, the last 3 of which are only useful in beacon-enabled networks. The active scan uses a beacon request frame with no source address and the destination set to the broadcast address (all ones) to extract a beacon frame from all coordinators within radio range.

During the scan, all frames received are discarded except beacon frames, which are passed up to the next higher layer either in aggregate or individually. When the scan of available radio channels is complete, the node sends an Association Request to the coordinator it has decided to join and waits for an Association Response. Coordinators may optionally assign a 16-bit short address to a node that can be used in place of the full MAC address in the Association Response.

It is worth noting that the role of coordinator has no meaning in peer-to-peer topology where short addresses not used, so neither does an Association Response with a status field that indicates success. How a device chooses which coordinator to join is out of scope for the standard, so under these circumstances the Association Request merely serves to set the state of the node, much like an IPv6 multicast address registration addressed to the all-routers broadcast address, which is always discarded by the router [8].

3.3. IPv6 Over IEEE 802.15.4
A typical 6LOWPAN network implicitly assumes a peer-to-peer topology where only data and (optional) ACK frames are passed at Layer 2 [9]. It is assumed that a PAN maps to a specific IPv6 link, to support link-layer subnet broadcast [10] by carrying multicast packets as link-layer broadcast frames. The standard accommodates the use of either IEEE 64-bit extended addresses or (after an association event) 16-bit short addresses unique within the PAN.

In the 6LOWPAN WSN the global IPv6 address is typically set through the process of Stateless Address Autoconfiguration [11] to avoid the overhead of having both a router and a DHCP server within radio range of every node.

3.4. IPv6 Stateless Address Autoconfiguration
Nodes begin the process by generating a tentative link-local address for an interface and joining the all-nodes multicast address and the solicited-node multicast address for the tentative address. The node then sends a Neighbor Solicitation (NS) message with the source set to the “unspecified” address (all zeros) to the solicited-node multicast address, to verify that this address is not already in use by another node on the link.

If another node is already using that address, it will receive a Neighbor Advertisement (NA) message on the all-nodes multicast address. A NS for the same target will be received if another node is simultaneously attempting to use the same address. The absence of these messages signals that the tentative link-local address is unique: the node assigns the address to the interface, and sends another NS message to the solicited-node multicast address with the source set to the link-local address. Nodes that receive this message respond with a unicast NA to the link local address of the sender that
includes their link-layer address. Thus a single request-response pair of packets is sufficient for both the initiator and the target to resolve each other's link-layer addresses.

The next phase of autoconfiguration involves obtaining a routable address prefix and selecting a default router. This process is slightly different using IPv6 Neighbor Discovery (IPv6 ND) [12] or the Routing Protocol for Low-Power and Lossy Networks (RPL) [13]. However, the essentials of the process are the same. Each router periodically sends advertisement packets to all-nodes multicast address, with its link-local address as the source. Hosts may send a request to generate an advertisement immediately rather than at the next scheduled time. Advertisements contain at least the prefix for configuring the full routable IPv6 address and a set of prefixes that identify on-link IP addresses. The node selects a default router, derives its routable (global or site-local) address using the prefix supplied, and sends a unicast message to inform the router that it is directly reachable via its link-layer (MAC) address. The router makes an entry for the node in its routing tables, and at this point both the router and the node have the address of the other in their neighbor cache.

Before moving on, we note that periodic NS-NA exchanges may continue in order to keep the neighbor cache up to date using Neighbor Unreachability Detection (NUD), particularly in networks where the higher layers do not provide confirmation that packets sent to a neighbor were received by its IP layer (UDP for example).

3.5. 6LOWPAN Header Compression

The final element that needs to be considered is header compression [14] since it relies on cross-layer packet information to reduce overhead and allow more data per packet. In the best case, IPv6 header can be compressed from 40 octets to two with link-local communication or seven octets when routing over multiple IP hops. This assumes (a) addresses assigned to interfaces will be formed using the link-local prefix or a small set of routable prefixes assigned to the entire 6LoWPAN; (b) the address IID is derived directly from either the 64-bit extended or the 16-bit short IEEE 802.15.4 address in the header of the encapsulating frame; and (c) the packet length can be inferred either from the Layer 2 "Frame Length" field or from the "datagram size" field in the 6LoWPAN fragment header (if present). Depending on how closely the packet matches this common case, some fields may have to be carried in full.

4. Methodology

Since forming a link-local address is the initial step in IPv6 network initialization and this is used in all of the other steps as well as header compression, the importance of the MAC address is clear. Obviously the address in the ROM of an interface cannot be changed, so if we want the MAC to carry global position coordinates it needs to be done before Layer 3 initialization. This requires: (a) a scheme for encoding the coordinates; (b) preconfiguration; (c) distributing location information; and (d) a method for supporting dynamic MAC address changes when a node refines the accuracy of its position location estimate.

The system described here is being implemented in Contiki-NG, the current version of the popular open-source, cross-platform operating system for next-generation IoT devices [15], which includes a simulator called Cooja. The default mac layer only handles data frames, and the design of the upper layers of the network stack is evidently driven by RPL, so the first step of implementation is some minor refactoring and adjustment of conditional compilation directives to create a simple IPv6 ND network with no routers, limiting the testbed to link-local communications.

A method for handling dynamic MAC address changes was developed by [16] as part of their implementation of the Moving Target IPv6 Defense (MT6D), which aims to prevent targeted network attacks by obscuring the communication between two devices through address rotation. That method was developed on the old version of Contiki, and simply treats the new address as a new node on the RPL network. This has the limitations of being tied to a particular RPL configuration and relying on garbage collection mechanisms, which the system described here overcomes by defining new ICMP message types.
4.1. Address Encoding

Tesseral addressing is a mechanism for labeling a n-dimensional shape which has been hierarchically subdivided (tessellated) into sets of same shape (isohedral sub-spaces), often referred to as tiles [17]. One way to do this is by interleaving the bits from the binary representation of row and column coordinates, a method commonly called Morton coding after the originator of their first use with geographic information systems [18].

To embed WGS84 coordinates in an IPv6 address, the first step is to map the integer parts of the coordinates onto a grid of 64,800 zones. The zone number is concatenated with 0xFD00 and the 40-bit Global ID to form the first half of the address. The bits of the decimal parts of the two numbers are interleaved to form a single 48-bit Morton code and put into the high bits of the Interface ID field. The 16 low order bits are reserved for an indicator of the transmission radius, which is the other key piece of information required for the trilateration calculations [1]. Since the convention for routing tables is to calculate the longest match on the high-order bits, using the zone as a subnet address facilitates routing and using the low-order bits for another purpose does not interfere. The process is efficient, requiring only five bitmask operations to encode or decode the coordinates.

The previous work used coordinates at seven decimal precision, requiring 48 bits; since this is beyond the actual precision of a GPS device, five digit precision is used which requires 32 bits. To embed WGS84 coordinates in an IPv6 address, the first six bits of the address are copied from the low six bits of the preconfigured PAN ID to signal the use of this encoding. The next bits are set to identify a locally administered unicast address, and the first 16 bits of the Morton code complete what would be the company ID in a globally administered address. In an EUI-64 address the next 16 bits are set to 0xFFFFE, so the first and last bits of this field are set to zero and one respectively to preclude confusion, and the remaining bits are used to carry the an indicator of transmission power and receiver sensitivity. While this breaks longest match semantics, if this information is replaced by a “helpful” radio (the enc28j60 driver in Contiki, for example) the minimum values specified in IEEE 802.15.4 can be used. The first 16 bits of the vendor supplied ID are the remainder of the Morton code, leaving four bits for flags and four “tiebreaker” bits that can be used to prevent duplicate addresses. One of the flag bits will signal a ground-truth node, the others are undefined at this point.

4.2. Preconfiguration

At the MAC layer, there is a non-beaconing peer-to-peer topology and no short addresses are used. The PAN ID is statically coded, and all nodes are configured to be coordinators. In effect, the PAN coordinator is assumed to be out of range of every node, making it invisible. It is tempting to use the zone (integer part of the global coordinates) as the PAN ID since it is a 16-bit field, but this would create two significant complications: there would be no way to identify overlapping networks run by different administrators, and it would not be possible to have a single network that crosses the boundary of zones.

Since the testbed is limited to link-local communications, at the IP layer all nodes are configured with the unique local unicast prefix and zone statically coded – information that would normally come from a router. In a real implementation “ground-truth” nodes must have their location coordinates set using a GPS device; in the testbed some selected nodes are configured with static coordinates.

4.3. Distributing Location Information

The easiest way to intercept packets is to put the interface into promiscuous mode, where every frame with a valid Frame Check Sequence (checksum) is passed to the next highest layer – in this case, the 6LOWPAN adaptation layer. However, simply listening on the channel as proposed in the earlier work consumes as much energy in one second as sending 35 broadcast or 58 non-synchronized unicast transmissions [19], so it is better to send a few extra packets to distribute location information.

Attempting to use the data exchanged during initialization creates a timing problem: since only ground-truth nodes initially have coordinates in their address, nodes on the periphery will be in an indefinite wait period while closer nodes calculate their position. A viable strategy is to have all nodes
join the network using their globally administered MAC address (from ROM), and respond to every NS they receive by sending a message to the all-nodes multicast address with a list of known nodes using coordinates in their address (which could be empty). Nodes that receive a populated address list (re)calculate their position coordinates, and if necessary, create new link-local and unique local unicast addresses and move to the address change routines.

4.4. Supporting Address Changes
In a simple IPv6 ND network address changes could be propagated using either the Redirect message, which is intended to be used by routers to inform hosts of the link-layer address of a better first hop for a destination, or unsolicited NA messages normally used for NUD. However, these may be useless for RPL configurations where the on-link neighbor cache is only maintained on the router rather than on every node. On balance it is simpler and more robust to define an address change message that includes the old and new address, rather than relying on the standard mechanisms to add the new address and let the old address time out of the cache, as is done in [16]. It takes the same amount of network resources to send an ICMP message with an experimental label as one with an RFC standard label, and the savings in terms of code from avoiding an extra message handler is negligible.

5. Results
The C library of functions for estimating the location of a node as the farthest point from which it can maintain communication with its neighbors, along with a finite set of (closer) alternative locations, and the library for creating a zone identifier and Morton code from WGS84 coordinates are complete and fully tested. The library functions for using the encoded coordinates in the IPv6 and MAC addresses are complete and fully tested with the transmission radius preconfigured as a single number. The required preconfigurations described in 4.2 above are unproblematic. The two new message types are currently implemented with UDP, and processing works as expected with custom data structures.

Several refinements will be finished in the immediate future. Transmission radius will be calculated by retrieving phyTXpower from the conceptual physical-layer PAN information base described in IEEE 802.15.4, and using a defined scheme for representing receiver sensitivity. An ICMP handler will be coded for the address change message and the NS response message with the list of neighbors, and the maximum size of the NS response message will be limited to the size of a single layer 2 broadcast frame.

Once that basic functionality is in place, timing needs to be investigated in a larger scale simulation to see how long it takes nodes that are farther from the ground-truth nodes to receive configuration information. The possibility of a “recalculation storm”, where nodes receive additional messages before they can finish processing the first one also needs to be tested, and other unanticipated wait/race conditions revealed. The testbed network will also be sufficient to baseline power consumption. Putting RPL back into the picture will be the final step for this phase.

6. Conclusion
This paper describes a unique low cost way to address limitations on determining directionality in broadcast networks using location-based addressing. Two inherent limitations of the overall scheme are worth mentioning. First, the accuracy of commercial GPS units mean this scheme is most appropriate when locating a node within an 8-11meter area is acceptable. A more significant feature is that every radio with the same neighbors will position itself in the same place, a weakness common to all algorithms of this class. However, since this one calculates a finite set of alternative locations there is scope for significant refinement with future work on calculating the most likely location given several sets of possible locations.
References

[1] O’Daniel, T, Hussein MN and Abdulla R 2018 Adv. Sci. Lett. 24 pp 1723–6
O’Daniel, T 2017 J. App. Tech. Innov. 1 pp 10–27
[2] IEEE Computer Society 2011 IEEE 802.15.4
[3] IEEE Registration Authority 2008 Guidelines for 64-bit global identifier (EUI-64
[4] Hinden R and Deering S 2006 IETF RFC 4291
[5] Hinden R and Haberman B 2005 IETF RFC 4193
[6] Carpenter B and Jiang S 2014 IETF RFC 7136
[7] National Imagery and Mapping Agency 1997 NIMA TR8350.2 (3rd Ed, Bethesda, MD)
[8] Vida R and Costa L 2004 IETF RFC 3810
[9] Montenegro G, Kushalnagar N, Hui J and Culler D 2007 IETF RFC4944
[10] Karn P, Bormann C, Fairhurst G, Grossman D, Ludwig R, Mahdavi J, Montenegro G, Touch J
and Wood L 2004 IETF RFC3819
[11] Thomson S, Narten T and Jinmei T 2007 IETF RFC 4862
[12] Narten T, Nordmark E and Simpson W 2007 IETF RFC4861
Shelby Z, Chakrabarti S, Nordmark E, and Bormann C 2012 IETF RFC6775
[13] Winter T, Thubert P, Brandt A, Hui J, Kelsey R, Levis P, Pister K, Struik R, Vasseur J and
Alexander R 2012 IETF RFC 6550
[14] Hui J and Thubert P 2011 IETF RFC 6282
[15] Kurniawan A 2018 Practical Contiki-NG (New York: Apress/Springer Nature)
Dunkels A, Gronvall B and Voigt T 2004 Proc. IEEE Conf. Local Comp. Nets (Tampa, FL)
(IEEE Computer Society) pp 455–62
[16] Zeitz K, Cantrell M, Marchany R, and Tront J 2017 Proc 2nd ACM/IEEE Int Conf. IoT Des.
and Imp. (Pittsburgh, PA) (ACM) pp 179-84
Sherburne M, Marchany R, and Tront J 2014 Proc 9th Cyber and Info. Sec. Res. Conf. (Oak
Ridge, TN) (ACM) pp 37–40.
[17] Shaffer C and Samet H 1990 Comp. Vision, Graphics, and Image Processing 50 pp 29–49
Coenen F, Beattie B and Shave M 1998 AI Rev. 12 pp 321–43
[18] Morton G. 1966 A computer oriented geodetic data base, and a new technique in file sequencing
Technical Report, IBM Canada Ltd.
[19] Gomez C, Kovatsch M, Tian H and Cao Z 2018 IETF RFC 8352