IP is Dead, Long Live IP for Wireless Sensor Networks

Jonathan W. Hui
David E. Culler
Outline

• IP’s and WSN
• Why prefer IPV6 over IPV4
• IPV6 Architecture
• Link Layer
• Network Layer
  - Neighbor discovery and Self Configuration
  - Forwarding and Routing
• Transport Layer
• Conclusion and Discussion
IP’s in WSN

• As WSN research took off, researchers denounced the idea of using IP in WSN as inadequate and contradictory to needs.

• Observation was: Sensor networks have different enough requirements, and warrant restructuring overall layering structure, application services

• The causes of disagreement/arguments:
  - Resource Constraints (limited memory, bandwidth, processing power, Energy)
  - A glut of unattended devices warranting self configuration.
  - Localized algorithms better suited to achieve robustness.
  - Naming would be data centric rather than identifying each node uniquely

With the advent of Active Message Dispatch ID being a replacement for the traditional header format, WSN diverted away from IP.

Since then, A series of protocols have been designed, which operate at link layer. But the requirement for a generalized abstraction still exist!

Since IP was discarded in the initial years of WSN, both IP and WSN have evolved through extensive research and practical deployments (WSN).
Contribution

- Develop an IPV6 architecture for WSN, which would allow end to end communication between nodes and IP devices at network layer.
- Develop a software architecture that preserves IP’s layered model, services, interfaces yet incorporate existing techniques developed in WSN community.
- Implementation of complete, efficient and production quality IPV6 solution, that can outperform existing systems, which do not adhere to any generic architecture.
IPV6 Architecture for WSN

• Why IPV6 instead of IPV4?
  Larger address space, but how much do we need!
  Autoconf feature, to auto configure Identification for glut of unattended nodes in the network.

Architecture:
WSN’s at the edge of IP networks, with all nodes assigned a common prefix (abstraction of subnet)

Connected to outside IP network through border routers.

IPV6 draws the abstraction of what principles to conform, the flexibility of Implementation mechanism, which facilitates the already working protocols models in WSN to be integrated, for the good.
Link Layer

The notion of IP Link:
The nodes reachable over a direct hop ie direct connection at physical layer.
WSN IP Link: Neighbors reachable over a single radio transmission

Properties of IP Link

Always on: Connectionless communication service to communicate with other nodes on the same link.

WSN emulation: Sampled listening forms the backbone for an abstraction of robust, always on IP link.

Best Effort reliability: Link must allow Best effort datagram delivery to network layer, using link layer retransmissions, and enable end to end mechanism for reliability.

WSN emulation: Synchronous acks, with extended capabilities (discussed later)
Link Layer emulation in WSN

Single Broadcast Domain: Allow Transitive reachability to all nodes on the link.
A -> B, B->C implies A->C

Avoiding contention: **MAC and MMC** (Media management Control)
Responsible for minimizing channel contention, by defining how to arbitrate access to medium in between transmissions.

**No single, widely accepted link layer protocol**, but the deployment of duty cycled protocol to improve energy efficiency is widely accepted.

MMC builds on B-Mac, WiseMac and employs a **combination of Sampled listening and Scheduling** to provide an efficient Link layer abstraction.
Link Layer in WSN ...

Sampled Listening:

required primitives: wakeup signal, channel sampling

Short chirp frames are used as wakeup signals.

The destination address and rendezvous time for synchronizing the wakeup time of communicating nodes, is embedded in chirps.

As we know from experience of X-Mac, these extensions solve the problem of unnecessary energy consumption due to use of long preambles, as well as overhearing.

Rendezvous time allows the receiver to turn off its radio until the time when data transfer is supposed to begin. This reduces the receive cost.
Link Layer in WSN ...

Synchronous Acks:

The conventional Ack frames have no addressing information, and could lead to false positives.

Unsecure and open to ack injection by attacker in sensible locations!

Ack frames couldn’t carry payload, which could be useful in feedback mechanism

The proposed new ack frame, is a data frame and thus could use the already defined mechanism for security, and can carry feedback information (useful for schedule optimization) as payload as well.

Scheduling and Streaming:

Nodes follow the concept of Localized Scheduling.

The ack messages contain scheduling information as sample period and phase. This would lead to reduced chirp transmission as nodes would synchronize more and more, with exchange of just one ack.

Leads to a reduced transmission cost.

**Frame pending bit could be set** to signal another incoming packet on the stream and reduce wakeup cost.
Adaptation and Compression

- IEEE 802.15.4 frame supports only 127 bytes of payload, whereas IPV6 has a 40 byte base header and 1280 byte payload.
- This results in introduction of an adaptation layer, which sits between the link layer and the network layer.
- Adaptation layer ensures the compression, fragmentation of IPV6 datagrams, to reduce transmission cost, and avoid redundant information transmission.

Header Compression:

Employs RFC 4944 header compression, which ensure stateless compression and thus gives flexibility to any of the neighbor nodes at any time.

The common values for IPV6 header fields, as version – 6, Traffic class – 0, Flow Label – 0, Next header – UDP/TCP/ICMP, IPV6 prefix could be assumed.

The redundant information as Payload length, Interface identifiers could be removed from IP header, as they could be derived from Link header.
Adaptation and Compression ...

- 6LP_IPHC compression uses encoding of 1 byte to hold compression state.
- 2 bits are used to distinguish 128 bit address carried, 64 bit interface identifier, bottom 16 bits of Interface identidfier, fully elided identifier. If the identifier is elided, it is assumed to be CGP or Link Local identifier.
- 1 bit : Version, Traffic class, Flow label elided or not
- 1 bit : next header elided or not
- 2 bits : hop limit, indicating whether 1 or 64255 or if carried inline

Compression Efficiency:
- 48 byte UDP/IPV6 header compressed to 6 bytes on link local unicast, 8 bytes on link local multicast, 11 bytes on global unicast within WSN, 25 bytes whne communicating with external IP device.
Network Layer (Neighbor discovery, Auto Conf, Forwarding, Routing)

Neighbor Discovery:

Nodes use it to detect each other's presence, neighbors link addresses, find routers and configure network parameters.

Border routers propagate Routing Advertisements to announce existence and disseminate network parameters.

Trickle algorithm is used to minimize overhead. The trickle timer resets whenever new parameters are discovered, or router solicitation messages are received.

RA’s are sequentially numbered according to update timestamp, so as to make sure that the nodes accept the most recent updates.
Auto Configuration

- IPV6 defines stateless and DHCP autoconf methods.
- Stateless autoconf: generates IPV6 address for a node by concatenating IID (derived from 802,15,5 link address), while Link Local Prefix is well known, the global prefix is communicated through RA message.
- The challenge of maintaining unique IPV6 address comes down to maintaining unique Link layer addresses.
- DHCP: Nodes contact a central server to request information.
- Since the server has a central view of the network, it ensures address uniqueness.
Forwarding & Routing

• Forwarding and Routing are explicitly different operations!
  • Forwarding:
    Next Hop Look up
  • Routing
    Forwarding table management
    Maintaining Default Routes
    Maintaining Host Routes

• Existing forwarder designs address throughput, fairness, high end to end success rate, but no effort to address energy efficiency.

• Hop by Hop forwarding rely on broadcasting and Snooping (costly in terms of energy Efficiency, due to increased listening time)

• Proposed use of Unicast Forwarder: applies hop by hop recovery, streaming and congestion control mechanisms for better efficiency and reliability
Unicast Forwarder

Hop by Hop Recovery:
- Link Layer acks and retransmissions on failures as queue overflows
- Network layer responsible for rerouting, rather than the link layer
- Next lookup operation independent to the routing updates running.

Streaming:
- Intentionally delays datagram forwarding, to reduce retransmission cost.
- Downside: Though Increased queue occupancy locally, and increased chances of packet loss at current node!
- Indicates whether more packets for the hop follow, thus improves overall channel utilization.

Congestion Control:
- Differing from usual norm, detects congestion when queue is full.
- Feedback mechanism to adjust data rates using additive increase and multiplicative decrease.
- Apply back pressure all the way to application Source

QOS
- Queue Reservation and different service to different class of packets.
Routing in WSN

- Responsible for establishing optimal paths by minimizing some routing metric.
- Work within the resource constraints of WSN: Limited memory, Energy.
- Reduced probing of neighbor nodes, and minimize the amount of routing information maintained and exchanged among the nodes, to improve Energy efficiency.

Implications:
- The nodes maintain partial routing tables, where the next hop for only a subset of destinations exist.
- The traffic for rest of the destinations, sent to the border router through a default root.
- The border router takes care of the routing logic, so as to ensure small routing information is maintained at the intermediate nodes.
Default routers

• Other than maintaining partial forwarding table, maintain a routing table as well for selection of default route to border router.

• Inserts potential routes in routing table, pin them in neighbor table as well to avoid being culled out.

• Uses PRR as Link quality estimate, each successful transmission updates PRR and builds confidence in the node.

• Sorts routing table according to hop count and confidence in Link quality estimate, and usually the first entry is chosen.

• Entries are removed from the table, when Link quality estimate drops below a certain threshold.

Minimal overhead in maintaining Link Quality Estimate:
A small section of live data flow is used to serve as Link Quality probes.
Maintaining Routing consistency

Routing information can become inconsistent at times, and would lead to loops or inefficient links.

Detection:
Forwarder tags each datagram with next hop’s expected hop count and ETX. Lesser than expected hop count signals possibility of a loop. Lesser than expected ETX value indicate that increased path cost has not been propagated.
Border Routers

- Hold a Global view of the network.
- Maintain host routes to every node in WSN, by learning the default route graph and reversing it.
- Default routers use RRO (Record Route Option), RRO contains addresses of hops that have forwarded the datagram.
- The destination path is then inserted in the datagram headers (which were transmitted on default route due to lack of entry in partial forwarding table), and forwarded to the destination by the border router.
- The overhead caused by RRO is minimized, as nodes who have just sent an RRO suppress their RRO transmission. RRO overhead scales with leaves and not nodes!
- Responsible for connecting WSN with outside network, talking to IP devices, if at all necessary!
- Use RA messages to propagate routing information to neighbor nodes, which hold the hop count and ETX for the node, relative to the border router.
Border Routers ...

- Multiple border routers would help reducing hop count for default routes.
- The border routers could communicate with each other, to exchange their subset of host routes.

Routing Overhead:

Default routers take just 64 bytes to maintain routing state.

Border routers are expected to have greater memory capacity, and the routing state overhead scales with the number of nodes.

Use of data traffic to estimate Link Quality estimate, minimizes control message overhead.

Transport Layer:

Since the lower layers conformed to IPV6 network Architecture, protocol layering, Best effort delivery, the implementation of TCP and UDP on top of it for end to end communication with IP devices quite straightforward.
Evaluation and Experiment Deployment

- Home monitoring Application deployed over a period of 4 weeks.
- Average duty cycle achieved : 0.65%
- Average per hop latency : 62 ms
- PRR : 99.98 %

But

Node generates one application packet per minute!

Does it stretch the network at all?

Transmissions are too little, which facilitate achieving duty cycle of 0.65%

Congestion highly unlikely!

Localized algorithm to detect congestion and apply back pressure

congestion control algorithm is not preventive and detected once congestion has actually happened, in case of massive data transfers does it hold well!
Goodput (Throughput) and Latency

- UDP: Link Local 9 kbps
  Over 3 hops 1.7 kbps
- TCP: Link Local 1.9 kbps
  over 3 hops 1.2 kbps
Evaluation ...

Is deployment of IPV6 worthy enough:
Provides layered abstraction
But...

- Massive packet payloads
- Added overhead of fragmentation and compression, decompression

Why can’t just the gateway router be IP enabled, and let the nodes speak their own language!

Security and Encryption may be necessary in some sensitive applications, but in others, it could just be an added overhead.