6LoWPAN

Based On-
IP is Dead, Long Live IP for Wireless Sensor Networks
-Jonathan W. Hui -David E. Culler
Presented By

- Milan Jain MT12067
- Anil Sharma MT12063
Outline

- Introduction
- Network Design And Software Abstraction
- Link Layer
- Adaptation Layer
- Network Layer
- Evaluation
- Application
- Can We Implement this in Flyport?
- References
Introduction

Internet of Things (IoT) and Wireless Sensor Networks
How This Started?

- **Core Internet** - Backbone routers and servers.
- **Fringe Internet** – Laptops, PC and local network infrastructure.
- **Internet of Things** – Low power, low-bandwidth wireless embedded devices.

Figure 1.2 The Internet of Things vision.
Internet Of Things (IoT)

- Uniquely identifiable things and their virtual representations in an Internet like structure.

- "The Internet Protocol could and should be applied even to the smallest devices"

- Low-Power devices with limited processing capabilities should be able to participate in the Internet of Things.

- Idea lead us to 6LoWPAN – "IPv6 over Low Power Wireless Personal Area Networks"
Evolution of Wireless Sensor Networks

- **Any vendor**
  - Price
  - Cabling
  - Cables
  - 1980s

- **Z-Wave, prop. ISM etc.**
  - Proprietary radio + network
  - Vendor lock-in
  - Complex middleware
  - 2000

- **ZigBee and WHART**
  - ZigBee
  - Open development and portability
  - 2006

- **6lowpan ISA100**
  - 6lowpan Internet
  - Increased productivity
  - 2008 ->

- **Scalability**
How 6LoWPAN different from TCP/IP?

<table>
<thead>
<tr>
<th>IP Protocol Stack</th>
<th>6LoWPAN Protocol Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application protocols</td>
</tr>
<tr>
<td>Transport</td>
<td>UDP</td>
</tr>
<tr>
<td>Network</td>
<td>IPv6</td>
</tr>
<tr>
<td>Data Link</td>
<td>LoWPAN</td>
</tr>
<tr>
<td>Physical</td>
<td>IEEE 802.15.4 MAC</td>
</tr>
<tr>
<td>Ethernet PHY</td>
<td>IEEE 802.15.4 PHY</td>
</tr>
</tbody>
</table>

- 802.15.4 at Physical and Link Layer – Duty Cycled Operations
- Adaptation Layer – Fragmentation and Header Compression
- Network Layer
  - IPv6
  - Layer two mechanisms – Bootstrapping, Discovering and Autoconfiguration

- Transport Layer
  - TCP not that useful.
- Application Layer
  - HTTP not much of use.

Will see in Evaluation
Primary contribution (Paper)

- Complete IPv6-based network architecture for WSNs that allows end-to-end communication between nodes and any IP device at the network layer.

- Software Architecture that preserves IP’s layered protocol model, defining the services, interfaces and their interaction that can incorporate many of the techniques developed within the WSN community.

- Implementation of a complex, efficient and production quality IPv6 solution for WSNs and show that general network architecture can outperform existing systems that do not adhere to any particular standard or architecture.
Introduction

• General argument by the Researchers in WSN research

“while many of lessons learned from Internet and mobile network design will be applicable to designing wireless sensor applications ... sensor networks have different enough requirements to warrant reconsidering the overall structure of applications and services”.

• Reasons IP is Dead for Wireless Sensor Networks
  • Resource constraints may cause us to give up the layered architecture.
  • Sheer number of these devices, and their unattended deployment.(Unreliable)
  • Limited task of sensing.
  • Traditional interfaces and layers of system abstractions should not be assumed.
Network Design And Software Abstraction

Network Design and Software Abstraction for IP
IPv6 Based Network Design

- Each WSN node serves as an IP router.
- As border routers forward datagrams at network layer, they don’t maintain any application layer state.
- Peers communicate in terms of the capabilities provided by the layer below.
- Link must allow network to achieve high “best-effort” datagram delivery.
  - To achieve reliable transport.

Figure 1.7 The 6LoWPAN architecture.
6LoWPAN with Traditional IP (Edge Router)
Software Abstraction

- Each node implements full network stack.
- It is to respect IP’s layered model while using the proper mechanism to support efficient communication in WSNs.
**IP Link**

- **IP Link** - Nodes that are reachable over single hop.
  - Direct Connection at Physical Layer.
  - Emulated over different physical communication domains.

- **Properties:**
  - Always-On
  - Best-Effort Reliability
  - Single Broadcast Domain

- **Problem:**
  - Places too much policy in Link Layer.
  - Network Layer unaware about complex link-layer dynamics.
Proposed Model - Avoiding IP Link Emulation

- Now, IP Link - Neighbors reachable within a single radio transmission.
- WSNs overlapping Link-local Scope.
- This violates *Single Broadcast Domain* Property.
- But provides better visibility into connectivity
  - Better Discovery and communication
  - Better control of forwarding policies.

Figure 1.13  A 6LoWPAN example.
Link layer

6LoWPAN
Introduction

• Low power radios consume as much power when receiving or just even listening when compared to transmitting.

• *Idle-listening* completely dominates system energy consumption when radio is not duty cycled.

• Industry has not yet come to agreement on a link protocol for duty cycled operation in Multihop Network.

• Developed duty cycle link protocol, while keeping in mind use of IPv6 network layer above (Interoperability).

• Duty-Cycled Radio – Transmitter can send packets to receiver at specific times.
Goal to Design Duty-Cycled Links

- Consume minimal power.
- Provides following IP-friendly properties:
  - **Always-On**: Nodes able to communicate without establishing connection or requiring any existing state.
  - **Low Latency**: Transmission delays to any neighboring node should be low.
  - **Broadcast Capable**: Able to broadcast frames to all neighboring nodes, regardless of node density.
  - **Synchronous Acks**: Link should allow IP to achieve high “best-effort” datagram delivery.
How They Achieved This Goal? - MMC

• MMC – Arbitrate access to media between simultaneous transmitters.

• Improve on WiseMAC by embedding addressing and timing Information into wakeup signal.

• Techniques Used:
  • Sampled Listening
  • Synchronous Acks
  • Scheduling
  • Streaming
Sampled listening

- Requires two primitives:
  - Wakeup signal when transmitting
  - Channel Sampling

- Chirp frame – 802.15.4 compliant frame and contains
  - Destination Address
  - Rendezvous Time: Time remaining until actual data frame transmission.

- Overhearing cost is reduced
- Rendezvous time allows destination to power down for that time.
- Reduces receive cost to that of receiving a chirp frame and the data frame.
Synchronous Acks

• Ack frame defined in 802.15.4 insufficient:
  • No addressing information.
  • Not Secured.
  • Cannot carry payload – Useful for hop-by-hop feedback

• New Ack Frame Defined as 802.15.4 data frame:
  • Addressing and Security mechanisms can be used.
  • Also carry payload which can be utilized for:
    • Scheduling Optimizations
    • Network Layer Optimizations
Scheduling

• Sample period and phase in payload of each ack.

• How it is helpful?
  • Node can synchronize to any neighbor after single acked transmission.
  • If destination’s schedule is known, chirp duration can be reduced to small synchronization guard time.

• Central Manager can be used: To collect and modify schedules of individual nodes.
Streaming

- To increase throughput and Energy Efficiency.
- Transmitter can signal that another data frame will immediately follow.
- Node can send data frames back-to-back without delay after sending a single chirp frame signal.
- This allows both sender and receiver to amortize wake-up costs across multiple frames.
Link Software Abstraction

- Link layer maintains neighbor table that holds link specific state about neighbors:
  - Link Addresses
  - Schedules
  - Frame Pending Indicator
  - Link Quality Statistics – Helpful in selecting routes
    - RSSI
    - Link Success Rates
- Also provides feedback on each transmission and reception.
  - Indicates whether transmission attempt was A ck ed.
  - RSSI of Ack.
  - Also RSSI for each received frames.
ADAPTATION LAYER

Fragmentation & Header Compression

Base header of 40 bytes and minimum MTU requirements of 1280 bytes

802.15.4 supports 127 bytes of payload and 80 bytes in worst case.
Answer - Adaptation Layer

- Header compression to support additional communication paradigms.

- Introduced header compression technique reduces 48 byte UDP/IPv6 header down to 6 bytes in best case.
Header Compression – RFC 4944 HC

- Stateless – provide nodes flexibility to communicate with any neighbor in compact form.
- Two ways to compress header
  - Making assumptions about common values for IPv6 header fields in WSNs.
  - By removing redundant information about layers.
    - Payload length and Interface Identifiers(IID) are derived from the link header.
- Doesn’t efficiently compress headers when communicating outside of link-local scope or when using multicast.
- When prefix is elided it is assumed to be CGP(Common Global Prefix) or Link-Local Prefix.
# IPv6 Header Compression

<table>
<thead>
<tr>
<th>VTF</th>
<th>Next Header</th>
<th>Hop Limit</th>
<th>Source Address</th>
<th>Destination Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>6LP_IPHC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![IPv6 Header Diagram](image)

IPv6 Header

Source address

Destination address
Packet Format (After Compression)

<table>
<thead>
<tr>
<th>VTF</th>
<th>Next Header</th>
<th>Hop Limit</th>
<th>Source Address</th>
<th>Destination Address</th>
</tr>
</thead>
</table>

• VTF (Version, Traffic Class, Flow Label) – 1 Bit to indicate whether elided or not.
• Next Header – 1 Bit to indicate Next Header is elided and 6LP_NHC is used.
• Hop Limit – 2 Bits to indicate whether 1, 64 or 255 or carried inline.
• Source and Destination Address (IPv6 Addresses) : 2 Bits each
  • Full 128-bit carried inline.
  • 64-bit IID carried inline.
  • Bottom 16-bits of IID carried inline.
  • Fully elided.
Compression Efficiency

• When prefix is elided it is assumed to be **CGP** (Common Global Prefix) or **Link-Local Prefix**.

• Possible compressions in various cases are:
  • Link-Local Unicast: 6 Bytes
  • Link-Local Multicast: 8 Bytes
  • Global Unicast: 11 Bytes
  • Multicast within WSN: 11 Bytes
  • Arbitrary IP Devices outside WSN: 25 Bytes
Network Layer

Forwarding And Routing
Why IPv6 for WSNs?

• Much **larger address space** *(128 Bits address).*

• Autoconf and ICMPv6 – Scalability, Visibility and Unattended Operations

• Inclusion of various two layer protocols e.g., ARP and DHCP into IPv6 framework.
Network Layer - Introduction

- Network Layer includes three services:
  - Configuration and Management
  - Forwarding
  - Routing

- ICMPv6 is used to configure and manage a large number of nodes in WSN.
  - Neighbor Discovery
  - Auto-configuration
Neighbor Discovery

- To detect each other’s presence and to find routers

- Routers periodically multicast RA(router advertisement) to announce their presence (operate over a single IP link, not multiple)

- Here RA is propagated to multiple hops with some network parameters

- Trickle algorithm is used to maintain freshness of information
Auto-configuration

- IPv6 support both stateless and DHCPv6 autoconf methods to assign unique address

- Stateless:
  - Disseminates parameters to all nodes (like using RA message)
  - Low cost (single RA message)
  - Global parameters?
  - Address generated by concatenating prefix with IID
• DHCPv6:
  • It selectively assign parameters to individual nodes (means behave like a central server)
  • Nodes request to central server for the unique address
  • Every WSN router act as a relay agent
Forwarding - Introduction

• Separate from routing.

• Responsibilities
  • Receive datagrams from an interface.
  • Next hop lookups in a forwarding table.
  • Submit message to appropriate interface.

• Primary Goal for forwarder design:
  • Energy Efficient
  • High end-to-end success rates.
Unicast forwarder

- Applies three orthogonal mechanisms:
  - Hop-By-Hop Recovery
    - Ensures that datagram will reach to destination
    - Link layer ack indicates whether or not network layer was able to accept the message.
    - So no need to rely on broadcast or continuous snooping.
  - Streaming
    - When submitting datagrams to the link, forwarder indicates whether other packets for the same next-hop destination follow.
    - If first transmission succeeds, it is likely that remaining transmissions will succeed.
    - Reduces average transmission cost.
  - Congestion Control
    - Congestion can cause queues to become full and decrease energy efficiency due to forwarding failures.
    - Uses feedback to adjust transmission rates using an additive-increase, multiplicative decrease control.
Quality of Service

- Previous three things may induce higher latency due to forwarding delays
- QoS allows upper layers to **select forwarding policy**.
- Three mechanisms:
  - Upper layer tag datagrams as latency tolerant:
  - Upper layer tag datagrams as high priority
  - Queue reservation for different traffic classes.
- Information about datagram is placed in an IPv6 Hop-by-Hop Option header.
Multicast Forwarder

• Simple controlled flood using Trickle.

• Trickle’s sequence number is included in an IPv6 Hop-by-Hop Option Header.

• Nodes buffer single datagram for continuous retransmission until maximum transmission period is reached.
Routing - Introduction

• Why Routing?
  • To establish reachability, forming paths, minimize routing metric

• Nodes are having limited resources like memory, processing power etc.

• Routing protocol for WSN
  • RSSI or (Link Quality information to detect PRR)
    • These measurements have high variance
  • Send control messages to compute PRR
    • Require more time, energy.
Because of limited resources
  • nodes have next-hop information for a limited set of destination
  • default route for all others

Border routers maintain host-routes to every node in WSN

Routing responsibility on border router reduces the control message overhead
Default routes

• Four main tasks

a) Discovering Routes
  • maintains a routing table (separate from forwarding table)
  • includes
    • Sender’s distance in number of hops
    • Estimated transmissions (ETX)

b) Managing the Routing Table
  • Router inserts potential route into the routing table
  • Selection by sorting the path cost and the link quality estimate
c) Selecting Default Routes
   • Top entry in the routing table is selected as the default route
   • Router randomly selects a small fraction of forwarded datagram for link quality estimate (uses hop count information)
     • No need to generate explicit control packets

d) Maintaining Route consistency
   • Can create loops or suboptimal path
   • Uses IPv6 hop-by-hop option
   • in case of inefficient routes RA Trickle timer is restarted
Host Routes

- Border router maintain host route to every node in WSN
- Border router routes the datagram to WSN node by inserting IPv6 routing header which contains path to the destination
- WSN node provide the default route information by including a RRO (Record Route Option) in IPv6 header.

- Inside RRO
  - contains a list of addresses, identifying the hosts that have forwarded the datagram.
- RRO requires 2 byte per entry
  - Because all have same prefix
Routing overhead

• Routing protocol configures both default and host routes

• Any communication overhead?
  • Broadcast from routers
  • Unicast from leaf nodes to border router

• Can we reduce this overhead?
  • by piggybacking on already existing traffic
Evaluation

Results Presented in the Paper
Hardware Description

• All the discussed techniques were implemented on TinyOS 2.x and TelosB platform

• TelosB
  • 16-bit TI MSP430 MCU
  • 48KB ROM, 10KB RAM
  • 2.4 GHz, 250 kbps TI CC2420 IEEE 802.15.4 radio
  • AES-128 authentication

• Evaluation of the Power Analysis of the IPv6 based network architecture
Experimental Setup

- The power model is validated in a real world Home Monitoring Application
- Data collection
  - Temperature, Humidity
  - Network Statistics
- Routing topology
  - 7 nodes within 1-hop of border router
  - Other within 2 or 3.
- Continued for 4 weeks
- Computed Average duty Cycle and success rate for each node
Evaluation Metrics

• Link Energy Cost
  • Total power consumed by the node

• Network Energy Cost
  • Average Power Draw in maintaining the connectivity of the network

• Application Energy Cost
  • Average Power Draw of a node in an application environment
Link Energy Cost

• Total power was modeled using listen, receive, transmit costs

\[ P_{total} = P_{listen} + P_{rx} + P_{tx}. \]

• How it was measured?
• Values of interest ...

\[ P_{listen} = P_{sleep} + f_{sample}E_{sample}. \]

\[ P_{rx} = f_{rx}E_{rx}. \]

\[ P_{txb} = f_{txb} \left( E_{tx} + E_{cb} + E_{cd} \frac{1}{f_{sample}} \right) \]

\[ P_{txu} = f_{txu} \left( E_{tx} + E_{cb} + E_{cd} \left( 2 + \frac{f_{\Delta}}{f_{txu}} \right) \right). \]

Any effect of chirp length?
Current Signature

(a) Channel Sample
(b) Receive Len=127B
(c) Transmit Len=127B
(d) Transmit Chirp=125ms
Understanding the Graph

- Transmission with chirp is more costly
- Why Transmit without chirp are more costly than Receive with chirp?
• Chirp length effects transmission

• Increasing sample rate reduces power draw when node is only listening

• Transmit with chirp is more costly than without chirp

• Transmit without chirp is more costly than Receive with chirp
Network Energy Cost

• Average power draw for a node maintaining network connectivity

• What is used to maintain connectivity of nodes?
  • RA (Router Advertisement) – Broadcast
  • RRO (Record Route Option) – unicast

• So what is the cost of transmission and reception?

\[
\begin{align*}
fr_x &= Nfra + Df_{rr} \\
ft_{xb} &= fra \\
ft_{xu} &= (1 + D)f_{rr}
\end{align*}
\]

\[
N = \text{Number of Neighboring Routers} \\
D = \text{Number of Descendants} \\
f_{rr} (\text{RRO unicast}) \\
f_{ra} (\text{RA broadcast})
\]
• In Case (a) - Transmit cost is more?
  • Because RA broadcast scales with the sample period (D = 5, N = 5).
• But not in case (b) (D = 0, N = 5).
  • Because no broadcast by host.
Take Away – Network Energy Cost

• Transmit is more costly than other operations

• Router nodes draw more power than Hosts
  • Due to broadcast of RA information

• Power draw increase when number of Descendants were increased

• Independent to number of neighbor nodes
Application Energy cost

• Average Power draw of a node in an application environment

• Both host-only and router nodes source UDP datagram to a data server through border router

• What was the overall cost?

\[
egin{align*}
    f_{rx} &= N f_{ra} + D (f_{rr} + f_{app}) \\
    f_{txb} &= f_{ra} \\
    f_{txu} &= (1 + D) (f_{rr} + f_{app}).
\end{align*}
\]

N = Number of datagrams by a node
D = Number of nodes to forward
• Why transmit power for Router Node is more than Host Node?
How Proposed System Is Better?

- Results were compared with prior deployments
  - RP – Report Period
  - DC – Duty Cycle
  - Latency – latency of the radio
  - DRR – Data Reception Rate
Goodput and latency

- **Goodput** - Application Level Throughput,
  - Number of information bits, delivered by the network to a certain destination, per unit of time

- Lower than UDP
  - Because TCP requires communication in both directions

![Graph showing Goodput and Channel Utilization](image)

(b) TCP Goodput

(a) UDP Goodput
Application

LessTricity – 6LoWPAN based Building Energy Saving and Management System
LessTricity system developed by consortium of companies in UK.

- **AIM:** Increase efficiency of energy usage and better management in commercial buildings and businesses.

- Uses wireless control and management technology based on 6LoWPAN to enable management of large facilities and even remote buildings.

Network architecture

- Small deployment consists of clusters of about 50 LessTricity power controllers (LPC).
- Each LPC transmits measured power through a 6LoWPAN network to LessTricity Network Interface (LNI-Edge Router).
- Readings are sent to a central database.
- A graphical web interface to monitor and manage energy consumption in the LPCs and to manage network and LPC themselves.

Figure 7.5 The typical network architecture of a LessTricity deployment.
Benefits from 6lowpan

- Easy Deployment.
- Compatible with building’s existing IT Infrastructure.
- Energy Usage information can be made available locally or over Internet for remote monitoring. Ex: Corporate Energy Usage Monitoring.
- **End User Focus:** Reduce energy footprint of their operations, both from cost saving and environment responsibility point of view.

| LessTricity application | | |
|-------------------------|------------------|
| SNAP                    |                  |
| UDP                     | ICMPv6           |
| IPv6 with 6LoWPAN       |                  |
| JenNet mesh layer       | IEEE 802.15.4    |

Figure 7.6 The Jennic 6LoWPAN stack with the LessTricity application.
Can We Implement 6LoWPAN?
Can we implement 6lowpan?

Wireless Sensors having 6LoWPAN Stack
Book Based on 6LoWPAN
– Zach Scelby
- Carsten Bormann
Thank You!!
QUESTIONS?
FEEDBACK/COMMENTS/SUGGESTIONS

6LoWPAN