University of St Andrews

CS4099

ILNP Routing for IoT

Author:
Jordan Mackie

Supervisor:
Prof Saleem Bhatti

April 2, 2019

1 NOTES

1.1 Fixing overhead

https://ieeexplore.ieee.org/document/7993954 to fix route reply storm issue:
add jitter before responding with route reply and listen for other replies
    select only works in windows NOTE
    Zoned Routing protocol Reverse Path Forwarding Woo

Abstract

Declaration

I declare that the material submitted for assessment is my own work except where credit is explicitly given to others by citation or acknowledgement. This work was performed during the current academic year except where otherwise stated. The main text of this project report is #TODO NN,NNN words long, including project specification and plan. In submitting this project report to the University of St Andrews, I give permission for it to be made available for use in accordance with the regulations of the University Library. I also give permission for the title and abstract to be published and for copies of the report to be made and supplied at cost to any bona fide library or research worker, and to be made available on the World Wide Web. I retain the copyright in this work.

Contents

2 Introduction

Despite the imminent exhaustion of IPv4 addresses [1], IPv6 is still being adopted slowly [2]. Brittle solutions such as NAT are being used to expand the IPv4 address space and to avoid the transition costs involved in upgrading to IPv6. Whilst IPv6 does expand the address space greatly and introduces functionality such as multicast, the internet protocol itself suffers from many issues.

2.1 Issues with IP

IP addresses are used both to identify a system and to determine its topological location. [3] lists several of the downsides to this overloading of IP addresses, and why the protocol was still used despite these concerns.

The separation of concerns that should be achieved by a layered model is not possible, since the IP address is used by the each layer in some way. IP addresses can be used in the application layer, and are bound to physical network interfaces, which goes against the end-to-end argument where each layer should provide a opaque abstraction to those above it.

The issues with IP are not just semantic. Due to the overloading of the IP address and the rapid increase in internet connected devices [4], the scalability of the system is being challenged. Implementations of multipath routing with the intention of balancing load is improving network performance for the operators that use them, but with IP it places greater stress on the default-free zone (DFZ) routing information base (RIB). Multihoming is also being used to improve reliability, but with IP this requires routing entries to store multiple addresses for one host. An IAB workshop [5] detailed how the DFZ RIB databases are growing in size exponentially due to the increasing number of devices and an inability to aggregate address prefixes. With IPv6 allowing for an even larger address space, this problem will only get worse.

Due to the growing number of Internet of Things (IoT) devices, mobility is also a necessary feature for a networking protocol. Mobile IP currently requires another entity (a home agent) to track and proxy packets to the mobile host as it moves from network to network. This mobility is also problematic for IPSec, which requires that the end system addresses remain fixed.

Given the difficulty involved in simply migrating from IPv4 to IPv6, it is

very doubtful that introducing an entirely different protocol for the internet would be successful. A backwards compatible solution would likely be the only solution that would be adopted within a reasonable time frame.

2.2 ILNP

Both multihoming and mobility are far simpler to implement and maintain if the identity and topological locator of a host are separated, and this is how the Identifier-Locator Network Protocol functions. [6] proposes ILNPv6, which implement ILNP with the same address space as IPv6 and the same packet structure as IPv6, but with different semantics for intepreting the addresses. ILNPv6 splits the original 128-bits used for an IPv6 address into two 64-bit fields: the upper bits representing the locator and the lower 64 bits representing the identifier. The version field in the IP header is used to differentiate between ILNPv6 and IPv6 packets, and routers that don't support ILNP can interpret the packets as IP without any issue.

The locator value identifies the subnetwork that a host belongs to, and a host can have multiple locator values, providing multihoming with smaller memory requirements for the RIB. The ID part of the address is unique to the host, and provides a fixed address which can be used at the transport layer.

Though ILNPv6 is very backwards-compatible, there are still some difficult challenges involved in its deployment. [7] describes how the tight coupling of the C socket API and IP addresses could cause issues in some legacy applications. ILNPv6 also requires some additions to the Domain Name System (DNS) to properly support multihoming.

2.3 Goal

The benefits of ILNP are clear for the entire internet infrastructure. The native support for multihoming and multipath routing is especially beneficial to typically mobile internet of things (IoT) devices. This project aims to exemplify these benefits for agricultural sensor networks in particular.

These devices are often restricted by limited battery life, memory, and computational capabilities. Most routing protocols focus on finding the shortest route between a source and destination, which often results in a small number of paths being heavily used and so some nodes are especially drained due to processing and forwarding of packets. This can result in a

network partion once crucial nodes fail (due to loss of battery), rendering a section of still operational nodes useless. By reducing the networking overhead and attempting to balance traffic across several paths, the network can remain operational for longer.

3 Context Survey

3.1 Internet Routing and Addressing Architecture

ILNP was listed alongside several other solutions to the current challenges facing the internet infrastructure in RFC6115 [8]. Locator-Identifer Split Protocol (LISP) also uses locator-idnetifier semantics and has already been deployed in 60 sites over 10 countries [9]. This ease of deployment is likely due to the fact that it requires no changes to hosts, and instead only required updates to core routers to be operational.

Another possible alternative is Routing Architecture for the Next Generation Internet (RANGI) [10]. RANGI again uses the identifier-locator split, but also has a cryptographic identifier which provides sender identification.

3.2 Energy Effecient Routing Protocols

Wireless sensor networks (WSNs) are typically very mobile with limited memory and power, and so require optimised routing protocols. Due to the myriad of situations that IoT devices are used, there is no one-size-fits-all solution.

[11] classifies diffeerent routing protocols and provides a survey of protocols for each class. Routing protocols are either:

1. **Proactive**, where each node maintains a routing table through knowledge sharing with adjacent nodes. Typically involves high overhead due to regular flooding, but performs better than reactive methods as mobility increases. Examples include AODV [12] and DSR [13].

2. **Reactive**, where nodes only seek out routes to remote nodes when one is required. Very little overhead in networks with low mobility, but performance degrades quickly as mobility increases. Examples include OLSR [14].

3. **Hybrid**, where features of both proactive and reactive protocols are used.

In typical internet infrastructure, it makes sense to use hop counts and delay as metrics for working out the 'best' routes to a destination. However, many protocol for WSNs also account for values such as remaining battery life, or how much computation the node is willing to commit to networking.

In order to save power, MAC layer protocols will often only listen for short intervals, or rely on lower power and lower bitrate receivers to fully wake the host when communication is occuring [15]. This behaviour is one of the reasons that reactive protocols are increasingly popular for WSNs, as they don't have the high risk of signal collision that comes with frequent updates.

3.3 IoT in Agriculture

The sensitivity of crops to changes in climate and agricultures crucial role on national economies has naturally resulted in large amounts of research and development. [16] describe how sensor technology is being used to monitor conditions in greenhouses, fields, and bodies of water. In order to make accessing this data more convenient and to help automate processes, they implemented a wireless network of enviromental sensors. These sensors communicate data to a gateway node which makes the data accessible via the cloud for visualisation and actuation.

[17] propose enviromental sensors but for urban environments with access to the cloud. By providing cheap montoring and actuating sensors to the general public, they hope to encourage healthier eating habits, as people would be able to grow their own vegetables effectively.

4 ILNP Testbed Implementation

Due to the recency of ILNPv6, there does not currently exist software for emulating ILNP networks as there is for the variations IP, therefore a custom testbed had to be implemented. This was achieved by building an ILNP overlay network using UDP with multicast.

A single UDP socket provided a communication endpoint. Sensors are initially unaware of each other, and so a simplified neighbour discovery mechanism is used to find which sensors are within radio range.

Since a mapping between the link layer MAC addresses and network layer IP addresses is used in IPv6 neihbour solicitation, and ILNPv6 can also use this mechanism, this was used to learn the IPv6 address of nodes that were also part of the multicast group. The grouping protocol discussed later involved one-hop packets to be broadcast, and so the IPv6 addresses could later be used for unicast communication.

5 Protocol Design

For this project a hybrid approach was used, based on the grouping protocol in [18]. By usinng a proactive link state protocol within groups of nodes and reactive protocols between, quick failure detection and recovery would be possible, without each node needing to understand the state of every node in the entire network. The approach taken could be referred to as a Zoned Routing Protocol (ZRP), where we have a intra-zone routing protocol (IARP) and a inter-zone Routing protocol (IERP).

5.1 Grouping Mechanism

When a sensor wants to join the network, it first broadcasts a query for what groups already exist around it (*HelloGroup*) . If no replies are heard after some duration, then it will declare itself the center of a group with a locator that could be assigned by some means. A configuration file was used in this case, but GPS could also be used in a real world example.

Neighbour nodes can reply with a *HelloGroupAck*, providing a value λ which can be used by the requesting node to choose which group it wants to join:

$$\lambda = \frac{AvailableConnections \cdot L + K_2}{MaxConnections} \cdot \sqrt{1 - \frac{E^2}{K_1}} \qquad (1)$$

where L is the % of load the node is willing to give to networking, E is % energy used (i.e. 0 is fully charged, 100 is empty).

If several groups are available for joining, the decision is made based on the highest average λ from each group. This discourages links forming with nodes that are under excessive load or are have little power left for forwarding packets.

After making it's decision, a node announces it's choice to all it's neighbours by sending a *OkGroup* message using the chosen groups locator value as the source locator in the ILNPPacket header. By informing nodes in the rejected groups also, a possible intra-locator next hop is established.

5.2   Intra-Zone Routing Protocol

Once a node has chosen and joined it's group, it joins in the process of sharing link state information. It's first links costs are established using the delay between *JoinGroup* and *JoinGroupAck* messages, as well as the λ values for its neighbours. These are combined to form a link cost:

$$C = \frac{T \cdot K_3}{\lambda} \tag{2}$$

Where T is the delay between sending the *JoinGroup* message and receiving an acknowledgement. When choosing the best next hop for a packet, the Floyd Warshall [19] algorithm was used, which provides the full cost of the shortest path between two nodes, as well as the next hop.

The link-state databases (LSDB) of the neighbouring nodes within the same locator are sent as part of the *OkGroup* message, updated to included the new node. The neighbours also broadcast this information to the rest of the locator group by using reverse path forwarding (RPF).

5.3   Inter-Zone Routing Protocol

6   Software Design

1. Component structure (socket interface, router/dsrservice/forwardingtable, raw sockets)

2. Runtime behaviour (packet parsing, routing, and forwarding)

3. Use figures to visualise project structure and workflow

7   Experiment

1. Discuss aim of experiment (to measure effeciency of the used routing protocol with ILNP, and compare to IP).

2. Explain case study, with reference to source (i.e. agricultural sensor setup)

3. Use visuals to show locators to real life position and sensor radi

4. Discuss experiment configuration (how machines were chosen, results collected, battery life simulated, etc)

5. discuss choice of metrics, justifcation and how to compare results.

8 Results and Discussion

1. Show heat map of results

2. Explain features of heat map

3. Describe the behaviour if IP was used instead through analysis

4. Discuss weaknesses with experiment

9 Conclusions

1. was the goal met, and if so how well?

2. future work with ILNP, possible suggestions of better alternatives to the routing protocol used.

10 Appendix

1. Instructions on installing, and executing and using the python module, and how to configure the experiments.

References

[1] RIPE NCC. Number of Remaining IPv4 Addresses. `https://labs.ripe.net/statistics/number-of-remaining-ipv4-addresses-daily`.

[2] Google. Ipv6 adoption. `https://www.google.com/intl/en/ipv6/statistics.html`.

[3] Brian E. Carpenter. Ip addresses considered harmful. *SIGCOMM Comput. Commun. Rev.*, 44(2):65–69, apr 2014.

[4] Statista. Number of connected devices worldwide in 2014 and 2020, by device (in millions). `https://www.statista.com/statistics/512650/worldwide-connected-devices-amount/`.

[5] Ed D. Meyer, Ed. L. Zhang, and Ed K. Fall. Report from the IAB Workshop on Routing and Addressing. RFC 4984, RFC Editor, September 2007.

[6] R. Atkinson, S. Bhatti, and S. Hailes. Evolving the internet architecture through naming. *IEEE Journal on Selected Areas in Communications*, 28(8):1319–1325, October 2010.

[7] Saleem Bhatti, Ditchaphong Phoomikiattisak, and Bruce Simpson. Ip without ip addresses. pages 41–48, 11 2016.

[8] Ed T. Li. Recommendation for a Routing Architecture. Informational 6115, Internet Research Task Force (IRTF), February 2011.

[9] Nahla Abid. *Design of a user-level naming solution for the future Internet*. Theses, Télécom Bretagne ; Université de Rennes 1, January 2015.

[10] X Xu and M Lu. *Routing Architecture of Next-Generation Internet (RANGI)*, pages 83–97. 01 2013.

[11] Noman Shabbir and Syed Rizwan Hassan. Routing protocols for wireless sensor networks (wsns). In Philip Sallis, editor, *Wireless Sensor Networks*, chapter 2. IntechOpen, Rijeka, 2017.

[12] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Experimental 3561, Network Working Group, July 2003.

[13] D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728, Network Working Group, February 2007.

[14] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). Experimental 3626, Network Working Group, October 2003.

[15] R. C. Shah and J. M. Rabaey. Energy aware routing for low energy ad hoc sensor networks. In *2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002 (Cat. No.02TH8609)*, volume 1, pages 350–355 vol.1, March 2002.

[16] T. Cao-hoang and C. N. Duy. Environment monitoring system for agricultural application based on wireless sensor network. In *2017 Seventh International Conference on Information Science and Technology (ICIST)*, pages 99–102, April 2017.

[17] G. Panda and T. Saha. Building of low cost reliable wireless sensor network for smart indoor agriculture products. In *2018 2nd International Conference on Electronics, Materials Engineering Nano-Technology (IEMENTech)*, pages 1–5, May 2018.

[18] J. Lloret, M. Garcia, F. Boronat, and J. Tomas. A group-based protocol for large wireless ad-hoc and sensor networks. In *NOMS Workshops 2008 - IEEE Network Operations and Management Symposium Workshops*, pages 7–14, April 2008.

[19] Stefan Hougardy. The floyd-warshall algorithm on graphs with negative cycles. *Inf. Process. Lett.*, 110:279–281, 04 2010.