University of St Andrews

CS4099

ILNP Routing for IoT

Author:
Jordan Mackie

Supervisor:
Prof Saleem Bhatti

April 5, 2019

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

1 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 has more intrinsic issues. The initial design for the infrastructure of the internet did not account for level of mobility that is common with network capable devices nowadays, and the attempts to retrospectively include support for such features have resulted in an incredibly complex system made of incompatible components.

1.1 Issues with IP and IoT

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 adopted despite them.

The separation of concerns that should be achieved by a layered model is not possible, since the IP address is used by 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.

As the number of Internet of Things (IoT) devices grows, mobility is also becoming 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.

IoT devices are often restricted by limited battery life, memory, and computational capabilities. Most IP 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. Mobility of nodes also requires more update messages to be flooded throughout networks. This can result in a network partion once crucial nodes fail (due to loss of battery), rendering a section of still operational nodes useless. A different approach to routing and addressing that reduced the networking overhead and attempted to balance traffic across several paths would allow IoT networks to remain operational for longer.

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.

1.2 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 interpreting 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.

1.3 Goal

The main goal of this project is to produce a library for a prototype communication protocol for Internet of Things (IoT) devices based on the identifier-locator approach.

By providing a libary for future developers and researchers to use, the adoptation of ILNP could be accelerated. The native support for multihoming and multipath routing is especially beneficial to typically mobile internet of things (IoT) devices, and so this project aims to exemplify these benefits for agricultural sensor networks in particular.

A sucessful implementation would include:

1. **Load Balancing**: The protocol will attempt to evenly disperse load across a network of IoT devices. This could be measured by demonstrating a reasonably even distribution of packets throughout the network of nodes when simulating sensor traffic.

2. **Soft Handovers**: The protocol will attempt to handle 'soft-handovers', allowing nodes to move between subnetworks and handle node failure without a noticeable effect on performance. A successful implementation will recover from failed nodes, with messages still arriving reliably. This could be tested by emulating network traffic, and triggering nodes in certain positions in the network topology to fail.

3. **IoT Optimization**: The protocol will account for battery usage on devices to reduce energy drain on devices. This will be tested through emulation of an IoT network and the energy cost of packets.

2 Context Survey

2.1 Ubiquity of IoT Devices

Despite the intitial motivation for WSNs being military applications, they are now being used to solve many other problems.

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. [8] 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. This data would then be collected at a sink node and could be analysed from an application.

WSNs currently often require specialised applications and manually specified network configurations in order for consumers to collect and analyse the data they produce. In order to make access to the data more standardised and easily available, research is also being done to connect sensor networks to the cloud. [9] propose enviromental sensors for urban environments with gateways to to the internet which could integrate into our own homes. 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.

[10] list the other applications of WSNs, and the different approaches to integrating WSNs and the internet. They recognise that providing a single gateway results in a single point of failure, and so focus on methods involving multiple or integrated gateways. This requires that sensors adopt the responsiblity of managing their networks topology instead of just forwarding towards a sink node.

2.2 Integration of WSNs and Current Internet Infrastructure

Previous research involving integrating WSNs into the current internet infrastructure is typically structured around IP. For all the reasons mentioned earlier, researches have realised the benefits of building WSNs using other approaches such as the locator-identifier split.

In RFC6115 [11], ILNP was listed alongside several other solutions that

resolved the issues faced by IP. One of the most well researched solutions listed is the Locator-Identifer Split Protocol (LISP), which has already been deployed in 60 sites over 10 countries [12]. Whilst it does not have natural support for network mobility, attempts have been made to provide it that require further extensions to the protocol [13].

ILNPv6 on the other hand has been able to demonstrate reliable mobility using a soft handover process [14]. Soft handover is where a host remains connected to it's original network while transitioning to a new one, which avoids loss of data when packets are still being routed to it's original network.

Soft handovers are crucial for high mobility devices such as smartphones, which are constantly transitioning between networks. Handovers are implemented in Mobile IP for IPv6, and has been improved since IPv4, but the method is still not as performant as it could be. It also further muddies the meaning of IP addresses, due to the use of different addresses (e.g. 'home' and 'care-of' addresses) in order to redirect packets to the mobile node.

A different addressing scheme is only part of the solution required for successful intergration of WSNs and the internet. IoT devices typically have limited memory and power, and so require optimised routing protocols if they are to be integrated effeciently. Due to the myriad of situations that IoT devices are used, there is no one-size-fits-all solution, and so many versions of IoT routing have been proposed.

2.3 Energy Effecient Routing Protocols

[15] classifies differeent routing protocols and provides a survey of protocols for each class. Routing protocols are either proactive, reactive, or hybrid.

Proactive each node maintains a routing table through knowledge sharing with adjacent nodes. Typically involves high overhead due to regular flooding and beacon messages, but performs better than reactive methods as mobility increases as links are repaired quickly. In the current internet, OSPF is one of the most popular interior gateway protocols, and so naturally researchers tried to adapt it to wireless networks. This produced the Optimized Link State Routing (OLSR) protocol [16] and Open Shortest Path First MANET Designated Routers (OSPF-MDR) protocol. Despite both making attempts to reduce enery consumption, they are defeated by reactive protocols in this area.

Reactive nodes only seek out routes to remote nodes when one is required. Reactive protocols involve very little overhead in networks with low mobility, but performance degrades quickly as mobility increases. Examples include AODV [17] and DSR [18]. Since these protocols were designed for mobile ad-hoc networks, most research involves improving the protocols awareness of energy availability. When a single node lies on many paths, it can be quickly drained by traffic, and so [19] produced a solution that considered the mean energy of a path before choosing which route to suggest to the requesting node. Reactive protocols also perform well in wireless environments as lack of periodic updates reduces the chance of interference which exists with link state proactive protocols.

Hybrid features of both proactive and reactive protocols are used. The hybrid approach is useful in scenarios where the grouping of nodes is appropriate. [20] use a clustering approach in order to manage resources within subsets of nodes. Since not all WSNs are homogenous, this approach can take advantage of some nodes having larger energy reserves than others by electing these nodes as the coordinator of the subnetwork.

3 Protocol Design

The protocol used is based on the Ad Hoc On-Demand Distance Vector (AODV) routing protocol, with added fields to try and account for energy usage. AODV is a reactive protocol which has three phases: discovery, maintenance, and recovery.

3.1 Discovery

AODV produces a list of hops that a packet can be sent over to reach a destination by flooding route request packets (RREQs). The route discovery process is summarised in figure 1, where the leftmost node (1) is requesting a route to the rightmost node (4).

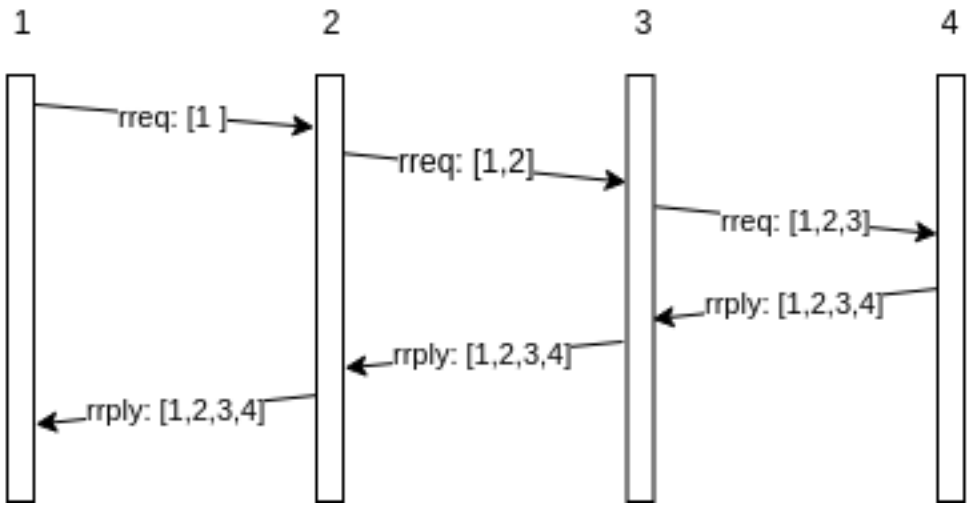

Figure 1: Route Discovery Overview

Figure 2 shows how RREQs are processed at each node. The destination node replies to all route requests for it, as this can provide multiple paths to the requesting node. Intermediate nodes however only forward requests based on whether or not they've seen them already. This can be established based on the request ID, which coupled with the source ID in the ILNP packet header can identify duplicate requests. Otherwise if this node's identifier already appears in the path so far, then it can also be discarded. These

checks reduce unecessary duplication of request packets and avoid loops in the resulting paths.

When using ILNP instead of IP with AODV, packets can be routed based on the identifier alone, and this can result in multiple paths to the same node. This provides robust communication if the end destination is multihomed (i.e. has interfaces to multiple locators), with less complexity than in IP. It also makes it easier to identify disjoint paths as the node has a single name in the network, which wouldn't be the case in IP multihoming.

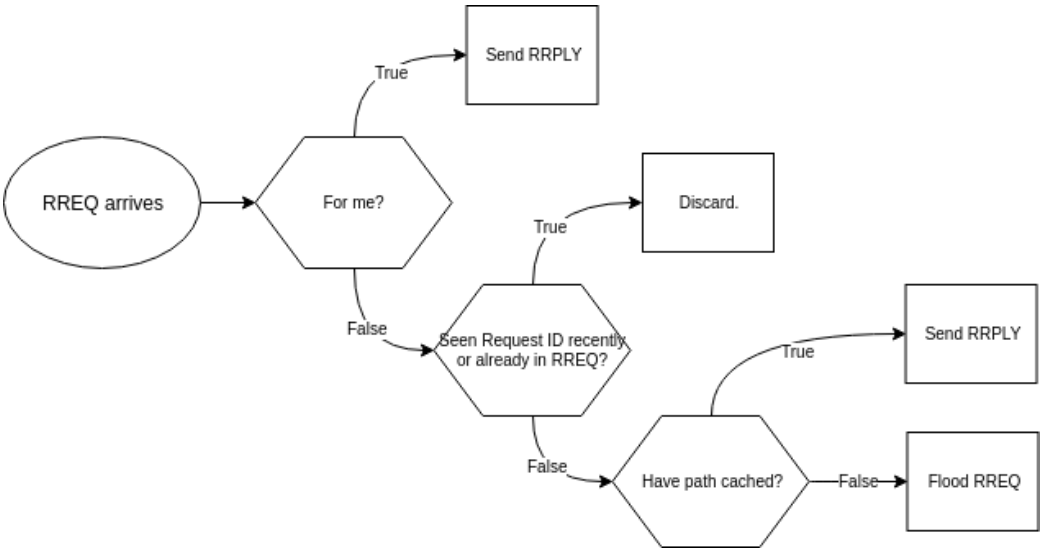

Figure 2: Route Request (RREQ) Flow

Once the RREQ reaches its destination, or any intermidiate node that already has a path cached to the that destination, a Route Reply (RRPLY) is generated by copying the full path from the RREQ or route cache and sending it back along the same path it arrived to the requesting node. Figure 3 shows the processing that occurs at each node.

By forwarding RRPLYs along the reverse of the path that they contain, we ensure that the route hasn't broken between creation and reception of the route request. Intermediate nodes can filter erraneous route replies by only considering those where they know the next hop neighbour is still available.

This only works if we assume that all links are bidirectional which is not always the case especially in heterogenous WSNs, due to differences in transceiver ranges. [21] shows that accounting for unidirectional links in

a protocol does not provide much benefit compared to the increased overhead. Also in our scenario, the nodes are likely to be homogenous and evenly spaced, so transceiver power can be assumed to be equal throughout, with no interference hot spots.

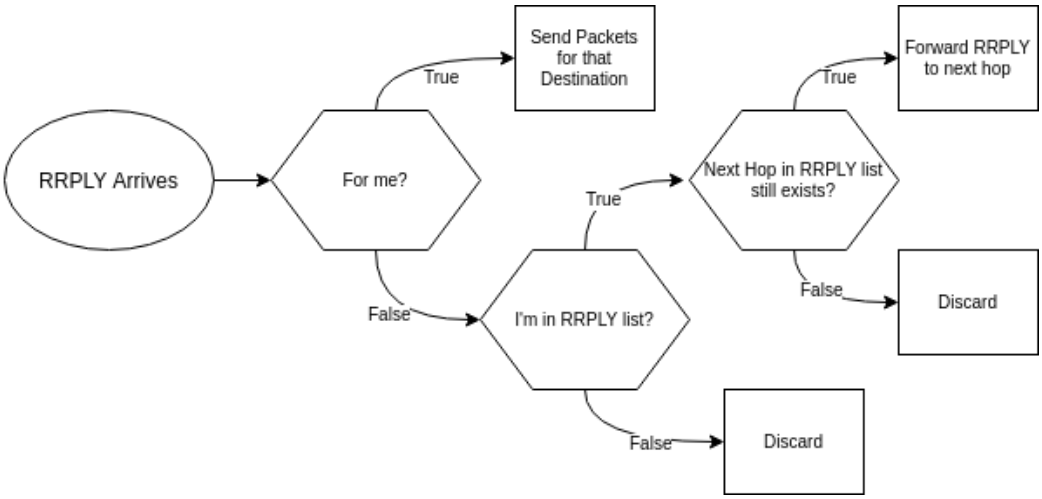

Figure 3: Route Reply (RRPLY) Flow

The structure of the route request is the same as in RFC3561 [17], but with an extra λ field in the header. This value provides a metric for determining the lifespan of a route, and is calculated for an individual node using equation 1, and visualised in Figure 4.

$$\lambda = 1 - (1 - E)^2 \tag{1}$$

where L is the % of load the node is willing to give to networking, and E is the % battery remaining. It is based on the equation for λ in [22], adjusted so that $E = 0$ occurs when the battery is empty. The effect of decreasing E was chosen so that the value of λ would be similiar during network initialization, but to avoid network partions smaller values of E would have a greater effect on λ. Each node calculates this value before adding their ID to the path in the RREQ, and only changes the field in the packet if its calculated value is lower.

[22] also included a load balancing factor that would account for the number of neighbours a node had, and this was considered for use in the AODV implementation. Instead of using the number of neighbours as in

their link state protocol, we could use the number of nodes using a route that passed through this node. This value could be ascertained by counting the number of unique source IDs of packets that were forwardded. However, defining a maximum in order to normalise this factor would place restrictions on how large the network could grow. Too large and the factor has no real effect, too small and it would reduce to zero making the metric meaningless for nodes further upstream. If this number could be supplied however, it would help other nodes choose routes that aren't being used as heavily, which would be very beneficial for the lifespan of the network.

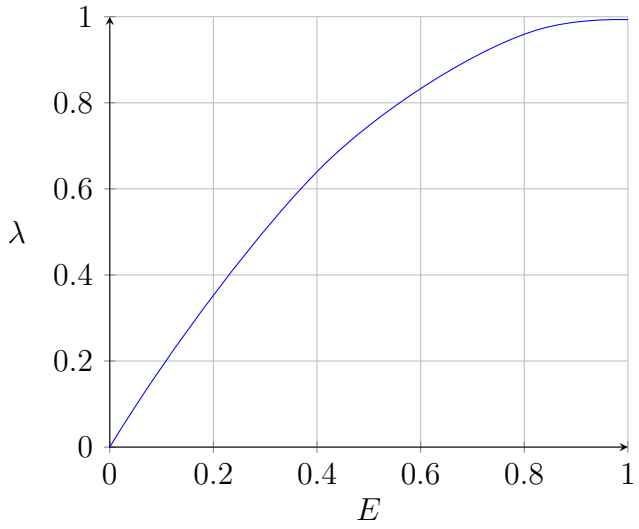

Figure 4: Plot of Equation 1

3.2 Maintenance

In order to check if neighbours are still live, *HELLO* messages are exchanged at regular intervals between neighbouring nodes. These messages also provide neighbour discovery as they are limited to one hop, therefore the source ID can be mapped to the arriving IPv6 address in the emulated link layer.

Figure 5 shows how the *HELLO* messages are processed. If a node fails to deliver a hello messages after a certain interval, then it's neighbours will begin the route recovery process.

Cached routes will also expire after some time to trigger another route request if required. This allows nodes to learn if a path is under heavy load,

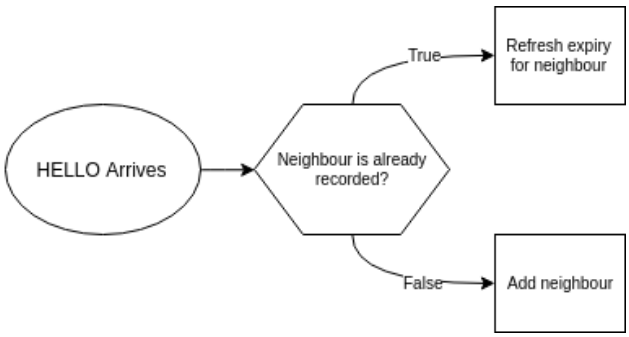

Figure 5: Hello Flow

and ensures that a route will be corrected if for some reason the recovery process is not completed.

3.3 Recovery

If the keepalive process fails for a neighbour, then a node will forward a RERR to all previous nodes in any paths it takes part in, shown in figure 6.

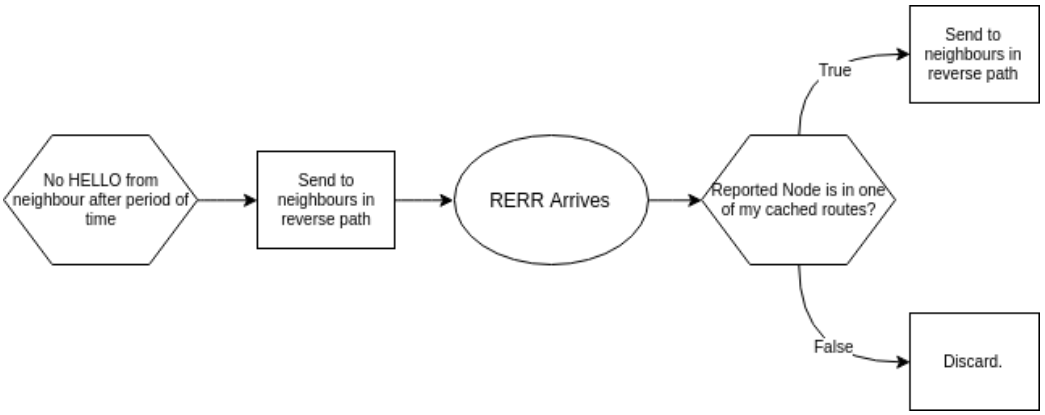

Figure 6: Route Error (RERR) Flow

Any packets that were sent between the failure of the link and the receiving of a route error will most likely be dropped, and future packets will be delayed as route discovery will have to take place again unless this node is aware of a disjoint path to the destination.

4 ILNP Testbed Implementation

Due to the recency of ILNPv6, there does not currently exist software for emulating wireless ILNP networks as there is for IP, therefore a custom testbed had to be implemented.

The testing environment was implemented using Python 3.7. The project has three main components: The wireless network emulation, routing and network management, and sensor emulation. Figure 7 shows the components with the flow of messages.

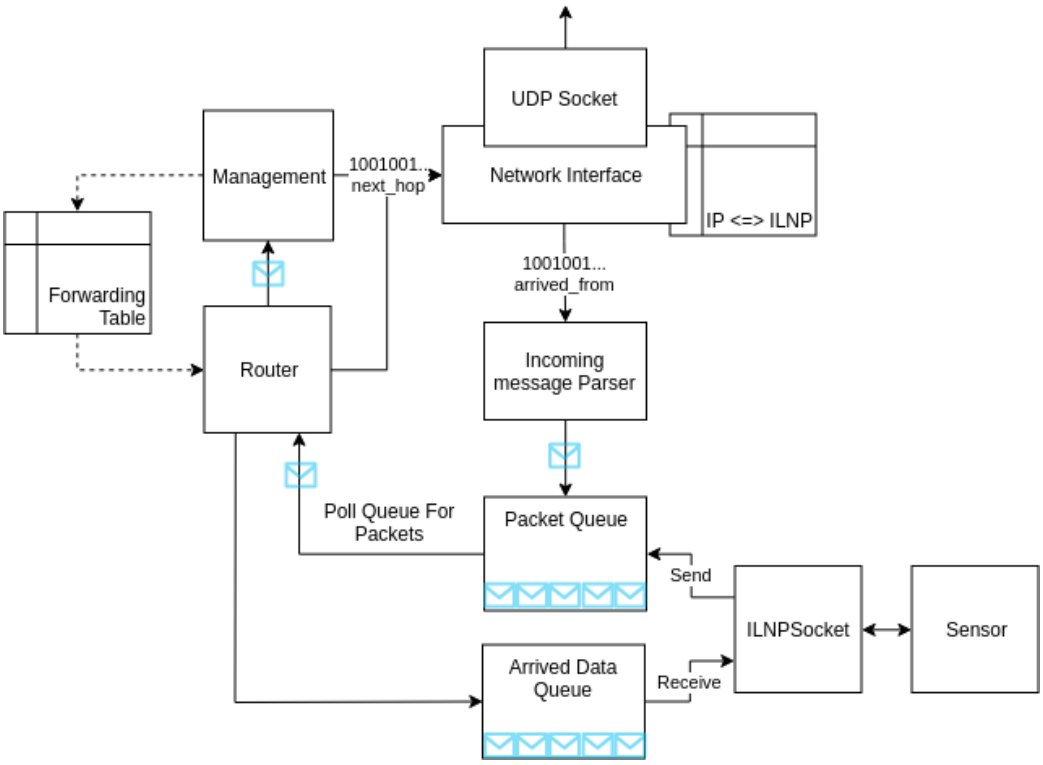

Figure 7: Implementation Structure

4.1 Wireless Network Emulation

Emulating wireless communication was achieved by building an overlay network using UDP with multicast. A single UDP socket provided a communi-

cation endpoint.

A multicast group exists for each node ID, and so neighbours of a node would join the multicast groups of their neighbours in order to receive broadcasted packets. Figure 8 shows the ranges of each sensors radio signal as dashed lines, where each node within the range joins the multicast group.

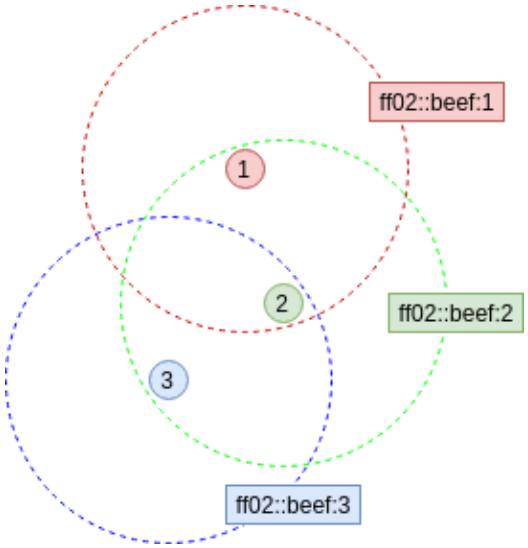

Figure 8: Wireless broadcast emulation using multicast

IPv4 uses the Address Resolution Protocol (ARP) and IPv6 uses Neighbour Discovery (ND) in order to produce a mapping between IP addresses and the link layer addresses of other machines in a local network. In our overlay network, the IP addresses of the underlying network could be treated as MAC addresses. This would allow us to emulate neighbour discovery in ILNPv6, and provide unicast communication once a mapping between these virtual link layer addresses and ILNP IDs were obtained via broadcasted messages.

The network interface abstraction provided the following methods:

1. **send**: For unicast communication.
2. **broadcast**: For establishing neighbours or flooding packets.
3. **receive**: For receiving packets, broadcast or unicast.

A daemon thread continuously polls the network interface for incoming data. It then parses the contents of the packet and records the source IDs and source IP addresses of any neighbourhood discovery packets for later communication.

All polling functions included a timeout in order for each thread to check if it has been asked to terminate, if for example the power levels had reached a critical level.

4.2 Routing and Network Management

The router polls the incoming packet queue and decides the next course of action using the processes described in section 3. The control plane handles any control packets or any packets that can't be forwarded using the current forwarding table.

TODO Finish description of control

#https://ieeexplore.ieee.org/document/7993954 to fix route reply storm issue: add jitter before responding with route reply and listen for other replies

4.3 Sensor Emulation

The sensor initialises the ILNPSocket, and depending on whether or not it is configured to operate as the sink (where all the data from every node is collected) begins either polling for packets or sending 'readings' at intervals.

To mock realistic application data, a random fluctuation is applied to a series of values that would be relevant in our scenario: temperature, humidity, pressure, and luminosity [8].

Only the ID of the sink is known by each node, which is all that should be necessary when using ILNP to route a packet. If it was possible to provide a FQDN for the sink node then the addressing scheme would be abstracted also, but emulating a DNS was deemed unecessary for the experiment.

5 Experiment

Multihomed sink provides simple multipath implementation

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.

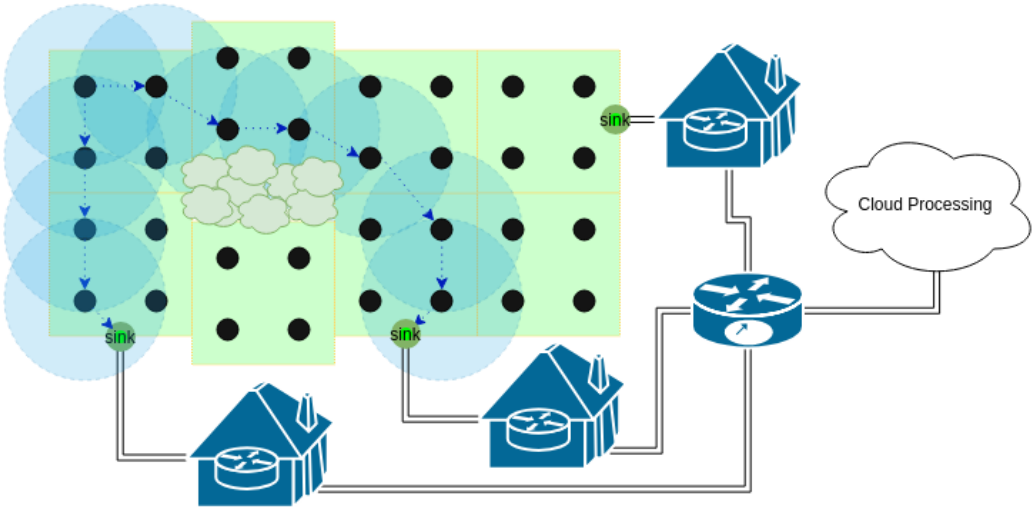

Figure 9: WSN layout with example route.

6 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

7 Conclusions

Improve AODV to use locator for 'approximate' routing, then complete path once reaches locator Mercy message to send from nodes under heavy load to try and request downstream nodes to use different paths.

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.

8 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] 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.

[9] 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.

[10] Delphine née Christin, Andreas Reinhardt, Parag S Mogre, and Ralf Steinmetz. Wireless sensor networks and the internet of things: Selected challenges. 01 2009.

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

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

[13] Z. Tang, Y. Zhou, W. Deng, and B. Wang. Lisp-hnm: Integrated fast host and network mobility control in lisp networks. In *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, pages 1–6, May 2017.

[14] Ditchaphong Phoomikiattisak and Saleem N. Bhatti. Network layer soft handoff for ip mobility. In *Proceedings of the 8th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks*, PM2HW2N '13, pages 13–20, New York, NY, USA, 2013. ACM.

[15] 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.

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

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

[18] 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.

[19] Jin-Man Kim and Jong-Wook Jang. Aodv based energy efficient routing protocol for maximum lifetime in manet. In *Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06)*, pages 77–77, Feb 2006.

[20] Shijun He, Yanyan Dai, Ruyan Zhou, and Shiting Zhao. A clustering routing protocol for energy balance of wsn based on genetic clustering algorithm. *IERI Procedia*, 2:788 – 793, 2012. International Conference on Future Computer Supported Education, August 22- 23, 2012,Fraser Place Central - Seoul.

[21] Mahesh K. Marina and Samir R. Das. Routing performance in the presence of unidirectional links in multihop wireless networks. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, MobiHoc '02, pages 12–23, New York, NY, USA, 2002. ACM.

[22] 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.