ACCEPTED FROM OPEN CALL

Performance of RPL Under Wireless Interference

Dong Han and Omprakash Gnawali, University of Houston

ABSTRACT

Smart homes and environments will consist of a large number of low power wireless devices such as sensors and actuators. Recently IETF standardized a network protocol called RPL that is designed to run on these nodes. In this article, we study the performance of RPL on a variety of scenarios that these nodes will encounter when they are deployed in practice. We deploy a network of 23 sensor nodes in a computer lab to monitor energy used by each computer across the applications and users. We subject the network to four different levels of interference that are representative of the types and levels of interference that these networks might encounter in deployment. Our study finds that RPL's reliability degrades even with an access point in overlapping channel under normal network traffic. With high interference, the packet delivery reliability goes down to 10 percent. The scenario that resulted in this performance is not unimaginable in smart home or environment. This performance degradation is partly due to lack of coordination across the layers of the protocol stack: RPL is unaware of the changes in the wireless environment underneath and proceeds as usual. As other research has shown, coordination across the network stack is essential for network protocols to work reliably in the presence of interference. This will require a more coordinated approach to standards across the bodies.

INTRODUCTION

One of the key enablers of smart homes and environments is low power wireless networks. Smart environments such as smart homes, offices, and factories envision that every object that makes the place functional or objects with which we interact might consist of sensing, actuation, processing, and networking capability. Smart environments may have hundreds or thousands of such nodes that work together to make our lives more efficient, comfortable, and safe. A smart home, for instance, could monitor occupancy and weather to control climate systems, schedule appliances at the most economical time of the day, make entertainment available in appropriate devices, and allow monitoring of energy use, security systems, appliance status, and even occupant activities securely through the Internet. Most of the nodes or objects in such environments use wireless network for relaying sensor readings to the controllers, relaying commands from the controllers to the actuators, and for nodes to communicate with each other depending on the application. One smart home can easily have several hundred wireless nodes.

As this vision gets ever closer to becoming a reality, it is time to do a reality check to understand if the wireless technologies proposed for such environments are up to the task. IEEE, IETF, and various industry alliances (e.g., ZigBee) have proposed and adopted standards for these networks keeping in mind constraints and properties relevant to these networks. Oftentimes, the nodes in these networks have limited power (energy harvesting, long intervals between battery change, or long operation of disposable smart objects). Thus, energy efficiency is one of the primary design objectives of such standards. IEEE standards such as various flavors of 802.15.4, IETF protocols such as RPL, and ZigBee all try to enable energy-efficient wireless communication between the nodes. One could power some of these wireless devices for a year or more with a single AA battery. The good news is these nodes are available for purchase today. While the progress in energy efficient communication in these networks has been nothing short of phenomenal, what is relatively unknown is how these networks might perform when they are deployed in massive numbers in the real world. There are two main networking challenges in such scenarios. The first challenge is inter-operation between the devices from different manufacturers that have products in different segments of the ecosystem that comprises the Internet of Things (IoT). The devices must have inter- operating MAC, networking, and application layers for them to work with each other. There is an emerging consensus that 802.15.4 type MAC, 6LoWPAN, and RPL will provide inter-operation at the MAC and network layer for the low- power devices, and standards such as ZigBee will build ontop.

The second challenge is to make sure these devices can co-exist with a large number of other devices. Is there enough bandwidth for all of them? Can they work despite interference from

RPL is designed for wireless networks such as sensor networks and networks in smart homes and offices that use low power devices. The predominant traffic pattern in these networks is multipoint-to-point, i.e., a large number of devices reporting their status and sensor readings to a server.

devices of similar type or different types? Researchers and practitioners have studied these issues for a long time most often coming up with a recommendation to run the devices in non-overlapping channels just to be on the safe side. This recommendation is a good common sense when we manually deploy a few access points in our offices or a few wireless nodes at our homes. When we deploy a massive number of nodes in smart homes or offices, we do not have that luxury.

In this article, we study the challenge faced by current standards in low-power wireless networks when they are deployed in a real world application. While there are prior studies that show how interference impacts various research protocols, this is a first look at the newly standardized RPL's performance under wireless interference in a realistic environment. We deploy a wireless sensor network that measures energy consumption of computers in a computer lab. The nodes use state-of-the-art standards for low cost wireless devices. The nodes have 802.15.4 compliant radios and run IETF RPL [1] protocol, with which they report sensor readings to a server. We subject the network to realistic interference from other similar devices and WiFi devices to understand the resulting performance of the network. We find alarming degradation in network reliability. This degradation is harmless in our application but in critical applications (such as security and occupant monitoring) would be unacceptable. With a detailed analysis of the network performance, we bring insights into the cause of this degradation. Thus we bring real world evidence to motivate future research and standards to address co-existence of devices in an increasingly wireless world.

Interference and Coexistence

A large number of smart devices for Internet of Things (IoT) operate on 2.4GHz ISM band. Most research on wireless co-existence naturally focuses on protocols and systems that operate in this band.

All networking professionals know to avoid overlapping channels to maximize the performance of a network. Unfortunately, we do not have this luxury as we deploy larger and larger networks. Many devices inevitably will operate on the same channel and cause interference to other devices in the same channel. In such a case, it becomes important to coexist with other devices. There are two types of interference a node must deal with: from the same type of device and from different types of device.

The same type of device employ the same protocol stack so it is easier to coordinate and accommodate transmissions across the nodes. However, if the devices using the same technology is sold by different vendors, it is possible that the devices use different configuration in their network stack making some devices more aggressive than others. One of the scenarios we study has a sensor node that aggressively sends a large number of packets drowning the rest of the nodes.

In a smart environment, most likely the wireless nodes encounter interference from many different types of devices. Bluetooth, ZigBee, and WiFi are three most common wireless technologies at homes. In this article, we study how devices running the latest IETF standard called RPL perform when they are deployed in such an environment.

Research in co-existence of devices running ZigBee or 802.15.4 compatible protocols and WiFi has been especially active in the last several years. In [2], the authors jointly consider the intensity and density of WiFi interference, then let the ZigBee nodes access the level of the local interference, and if necessary switch to a new channel.

It has been shown that existing CSMA mechanisms are inadequate to enable Zigbee to coexist with WiFi [3]. The authors show that modeling and predicting the length of space in WiFi traffic allows setting the right frame size in ZigBee to maximize throughput. The experiments on real hardware using testbed demonstrated the proposed control protocol enabled ZigBee nodes to communicate reliably even under heave WiFi interference. Other researchers have shown that it is possible to make communication reliable despite ZigBee-WiFi interference using header and payload redundancy [4].

These and many other research projects explore techniques for coexistence between same and different devices. They are slowly being discussed at the standard bodies and none of the devices available in the market today employ such technologies. In this article, we use the latest IETF routing protocol called RPL, which is designed for low power wireless networks, and understand how it works when it is run on top of 802.5.4 compliant radio in presence of different levels and types of interference.

Routing in Low-Power Networks Using RPL

RPL is an IPv6 routing protocol for low power and lossy networks recently standardized by the IETF in RFC 6550 [1]. RPL is designed for wireless networks such as sensor networks and networks in smart homes and offices that use low power devices. The predominant traffic pattern in these networks is multipoint-to-point, i.e., a large number of devices reporting their status and sensor readings to a server. Such routes are established by forming a directed ascyclic graph (DAG), an implementation of a distance vector protocol. The packets are forwarded along the DAGs which span the whole network. Each non-leaf nodes in the DAG will act as a router, potentially be a parent node on a path towards the root of DAG. The nodes use Objective Functions (OFs) to select parents within an RPL instance. We choose OF0 in our experiment, which uses hop-count as the metric to select parent and path. RPL also supports sending messages from the root to individual nodes. Such messages are used to control the devices such as lights, appliances, and power strips.

RPL could potentially be deployed in homes, offices, factories, and even at the edges of smart-grids as part of advanced metering infrastructure

on devices like smart meters and electrical appliances. Although this standard is less than one year old, there is a huge interest in understanding how RPL works because the scope for its application is so wide.

Researchers have used simulations and real-world experiments to understand the performance of RPL. Simulation studies of RPL have shown how quickly RPL can establish routes in the network however has large control overhead [5]. Other studies have shown RPL to have performance comparable to ideal shortest path routing [6]. A different study in simulation showed that RPL lives up to its promise of efficiency in energy, storage, and communication overhead [7]. A study of point-to-point routing in RPL found inefficiencies [8]. The IETF has addressed these issues by defining a more efficient point-to-point routing mechanism for RPL. RPL has also been studied as a part of a stack with CoAP, an HTTP-like protocol for constrained environments. The study found RPL to work well as a networking substrate [9].

Experiment Setup

Our goal is to study the performance of a network running RPL under various levels of interference such networks could encounter when they are deployed in the real world. We now describe experiment setup that we used for this study.

Application

We deployed an application to monitor the power use of computers in a computer lab. The lab has 23 computers arranged in four rows. The students can log in to these computers to check emails and do their homework. The goal of the application is to closely monitor the energy used in a time scale that helps us uncover the trends used by different computers, applications, and students. This application has been running continuously for five months.

Network

Figure 1 shows the network architecture. We use PowerNet [10] nodes as the energy sensor nodes, which are attached to the computers in series between the power cable and power outlet. The PowerNet node has energy metering IC to record energy being supplied to the computer and report it to the server. It has CC2420 radio, which provides the IEEE 802.15.4 PHY layer. At the MAC layer, we use TKN15.4 [11], which is an implementation of IEEE 802.15.4-2006 MAC layer but without the support for security services, PAN ID conflict notification and resolution, and frame buffering in transaction queue after CSMA-CA algorithm fails. We use the TinyOS RPL implementation which consists of Blip, the TinyOS 6LoWPAN stack, and TinyRPL, an implementation of the RPL standard [12]. Blip implements 6LoWPAN header compression, 6LoWPAN neighbor discovery and DHCPv6. Hop-by-hop retransmissions are used to improve packet delivery reliability. We use a Tmote node as the gateway, which also runs RPL. We attach the gateway to a Unix server through a USB port. The gateway receives and forwards all of the incoming packets to database for further analysis.

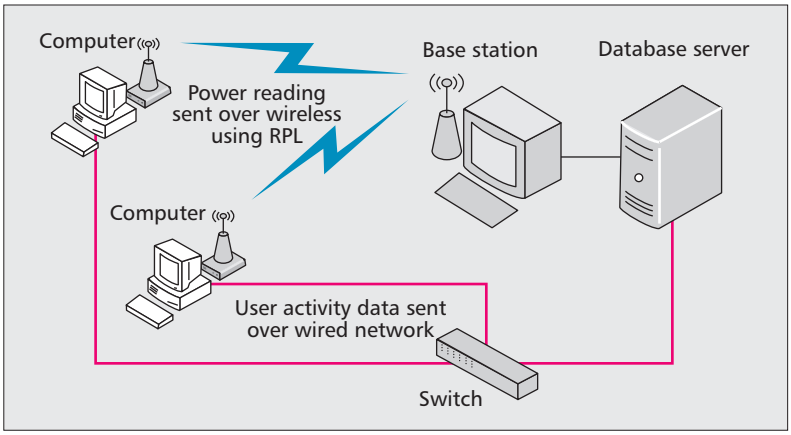

Figure 1. *Architecture of a sensor network deployed to monitor energy used by computers.*

Instrumentation

The nodes sample power at 10Hz, pack 20 readings to a single packet and send it to the base station. In addition to the application payload, the packets contain other metadata that we later use to analyze RPL information. Every minute, the nodes also send summary of data and control plane counters for further analysis. With this set of information, we can study RPL's performance at the network layer and also able to drill down to MAC layer mechanisms to explain the performance (number of retransmissions, number of times route changes, received signal strength, etc.) at different time scales.

Scenarios

We designed four experiment scenarios with different levels of interference:

- *Low Interference*: We set the PowerNet nodes to run on 802.15.4 channel 25, which does not overlap with any WiFi channels in the United States. We verified that this channel was free of interference. The only interference is due to other PowerNet nodes.
- *Normal Interference*: In this scenario, the PowerNet nodes run on 802.15.4 channel 12. This channel overlaps with WiFi channel 1. In the department, there are several APs that use this channel. This scenario represents the most common case of interference due to the normal use of Wireless AP on overlapping channels.
- *Mixed Interference*: In this scenario, in addition to running PowerNet nodes on channel 12, we put two low power nodes on 802.15.4 channel 12. These two nodes were programmed to send packets to each other as quickly as they can with maximum power. Thus the PowerNet nodes experience interference not only from WiFi AP but also the traffic bouncing between these two nodes.
- *High Interference*: In this scenario, we deployed an additional WiFi AP in the lab and configured it to run on channel 1, thus overlapping with the channels of public APs and PowerNet. Then we connected to this

AP using a laptop and generated continuous traffic at 20 Mbps using Iperf. Thus, the PowerNet nodes are subjected to high interference from WiFi as well as 15.4 in this scenario.

We ran the network for 10 hours in each scenario in the same time of day to get repeatable results.

RPL'S PERFORMANCE UNDER INTERFERENCE

We subject the energy monitoring network running RPL to various levels of interference to study RPL's performance. In this section we present our findings.

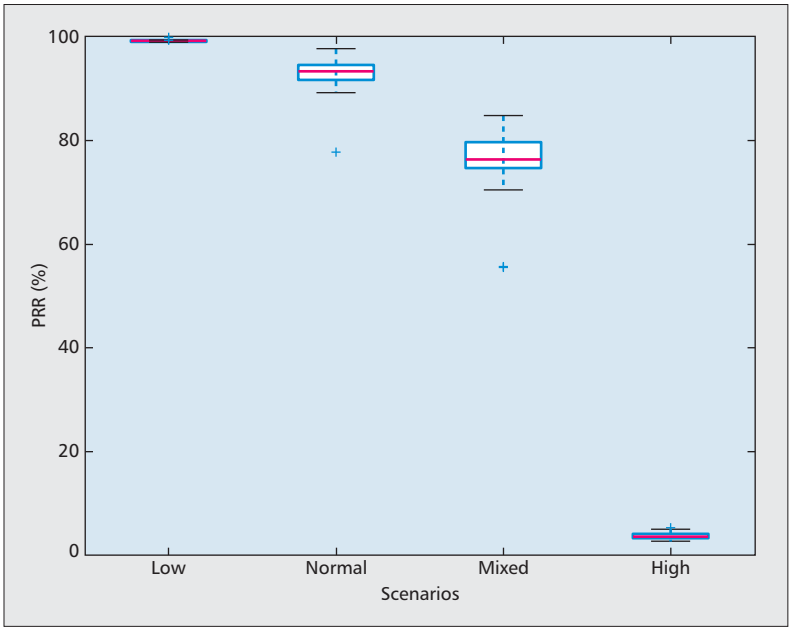

Figure 2. *Packet reception rate under various interference scenarios.*

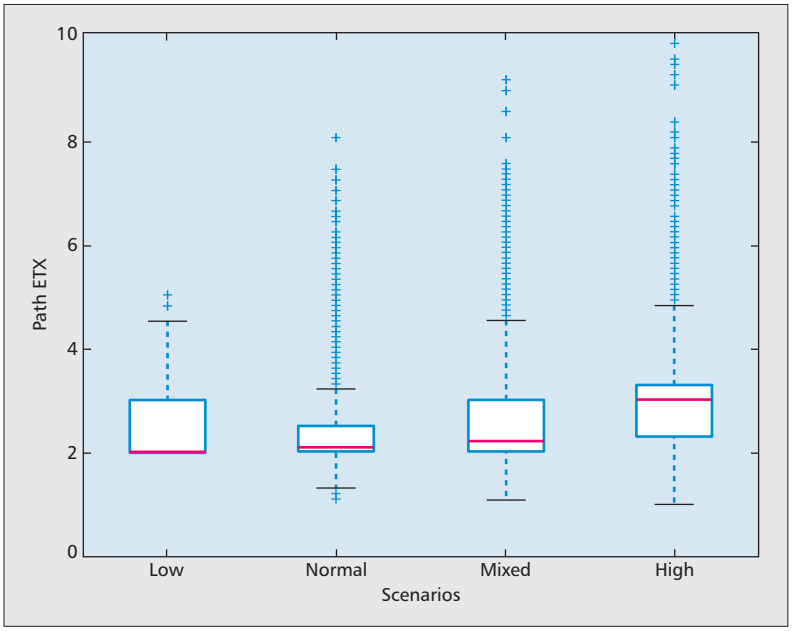

Figure 3. *Path ETX under various interference scenarios.*

RELIABILITY

We want our network to deliver packets reliably. While some applications might tolerate some losses, critical home monitoring applications cannot. Packet Reception Rate (PRR) is the most common metric used to quantify how reliably a protocol can deliver packets to the destination. We expect each link chosen by a good routing protocol to be reliable but that is insufficient for successful multi-hop forwarding: the entire path needs to be of high quality. So, we use the end-to-end version of the PRR metric, i.e., what fraction of the packet that was sent arrived at the destination which is multiple hops away.

Figure 2 shows the average PRR for each scenario. The PRR stays at almost 100% with low interference and about 92% with normal interference. When there are WiFi and 15.4 nodes interfering with PowerNet, the PRR drops to an average of 75%. In the last scenario, i.e., high interference, the average PRR of the nodes drop to below 10%. The figure shows that under normal interference, the performance of RPL might be acceptable but when there is high interference very few packets are reliably delivered.

To explain this trend in reliability in more detail, we analyze the quality of paths selected by RPL for forwarding the packets in each case. We use the metric called Path ETX to quantify the quality of path. Path ETX is the expected number of transmissions and retransmissions required to deliver a packet from a source to the destination over multiple hops.

Figure 3 plots the distribution of path ETX in each scenario. In low interference scenario, almost half the paths have ETX of 2, and most distributed in the 2-3 range. The Path ETX increases, but only slightly with normal and mixed interference. There is a larger increase in Path ETX with high interference. Almost half of the paths have ETX of 3 or larger and 10% of the paths have an ETX of 4 or larger. Thus, worse paths become more common with higher interference and cause lower packet delivery.

CONTROL OVERHEAD

Control traffic is used to discover, setup, and maintain the routes in the network. RPL uses adaptive timers to adjust the rate at which the control messages are sent. The efficiency is achieved in a long-running stable network where the control traffic might be sent once every several hours. We normalize the number of control packets sent by the number of data packets to obtain control overhead ratio, i.e., how many control packets are sent for each data packet in the network. RPL is designed for low power networks to provide efficient communication so we expect its control overhead ratio to be low.

Figure 4 shows the control overhead ratios across the four scenarios. With low interference, the control overhead ratio is distributed in the range of 15% to 20%, i.e., RPL sends 0.15 to 0.2 control packet for each data packet. With normal and mixed interference the control overhead ratio increases to about 30% and 50%

respectively. This shows that with increasing interference, RPL needs to work harder to discover and maintain viable routes for data delivery. With high interference, the ratio increases to almost 100%. This is most troubling because RPL is sending almost one control packet for each data packet delivery. The high control overhead ratio is due to the larger number of control packets being sent and much lower number of data being sent successfully when there is high interference.

Network Churn

As RPL discovers better paths or discontinues using a bad link, it switches to a different preferred next hop (or parent) for a given destination. This process not only changes the next hop but could also change the Rank. RPL use Rank to approximately (depends on the routing metric) indicate the hop distance of a node from the root of network. The larger the rank value of a node, the longer the path from the root to the node. An unstable network changes the routes many times. When RPL selects a new route, it does not necessarily change the node's Rank because the new route might also be of approximately the same length.

Figure 5 shows the number of parent changes for the four scenarios. With low interference, the network is stable: each node changed the parent 1.7 times per hour in average. We see more frequent parent changes with normal and mixed interference. With high interference, each node changed parent 1400 times per hour in average. This suggests that when there is interference, the adaptive Trickle timer was reset many times which causing the node to send a large number of control packets. These numbers tell us the nodes change parents more often when there is interference but does not tell us if these changes result in finding substantially different paths. To study the network churn in more detail, we define a new metric called Excess Parent Change (EPC) defined as Eq. 1:

$$EPC = \frac{Num.ParentChange - Num.RankChange}{Num.RankChange} \quad (1)$$

The EPC metric helps us discern between the two cases — a node changes parents when it discovers a better or worse path (according to Rank) or when it changes between multiple parents without any significant change in Rank. The latter could occur when a node switches between many parents without improving the Rank, e.g., when it is subjected to interference.

Figure 6 plots the Excess Parent Change (EPC) metric. The rare interference scenario has almost no excess parent change, i.e., almost every time the node changes the parent, it also changed Rank. With high interference, the EPC is between 30 and 60 percent. This indicates that 30–60 percent of the time the parent change resulted in no change in Rank, thus resulting in no improvement in path quality.

This result together with the high control overhead indicates that although RPL works harder it does not find better paths when it is subjected to high interference.

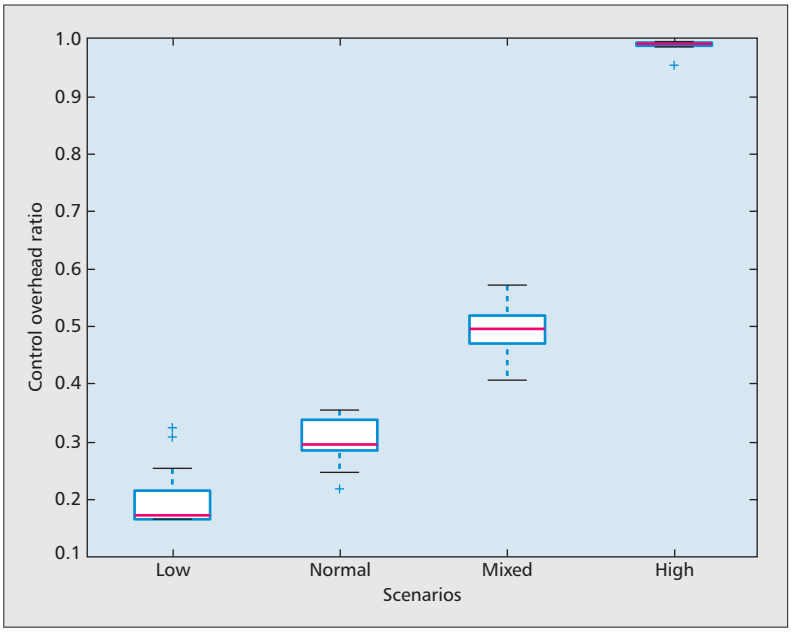

Figure 4. *Control overhead ratio under various interference scenarios.*

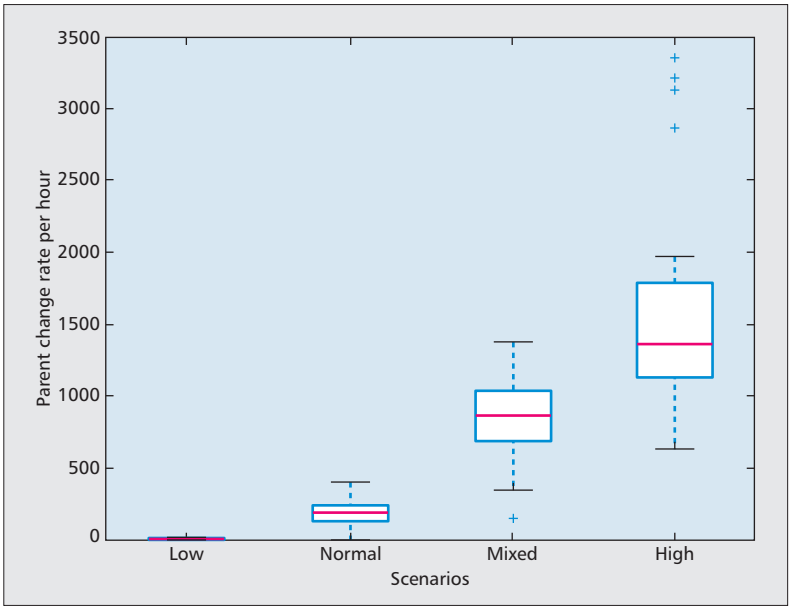

Figure 5. *Parent change rate under various interference scenarios.*

Discussion

Although our results show RPL performing poorly with interference, the results somewhat depend on the values of the configuration parameters chosen in the implementation. We use the defaults in the TinyOS implementation of RPL. It is certainly possible to tweak the parameters to make RPL work better in a specific environment. However, parameter tweaking is tricky, especially in protocols like RPL that is expected to be deployed in a wide range of settings. The qualitative results will still hold because of the way today's network stacks are designed.

RPL's poor performance under performance

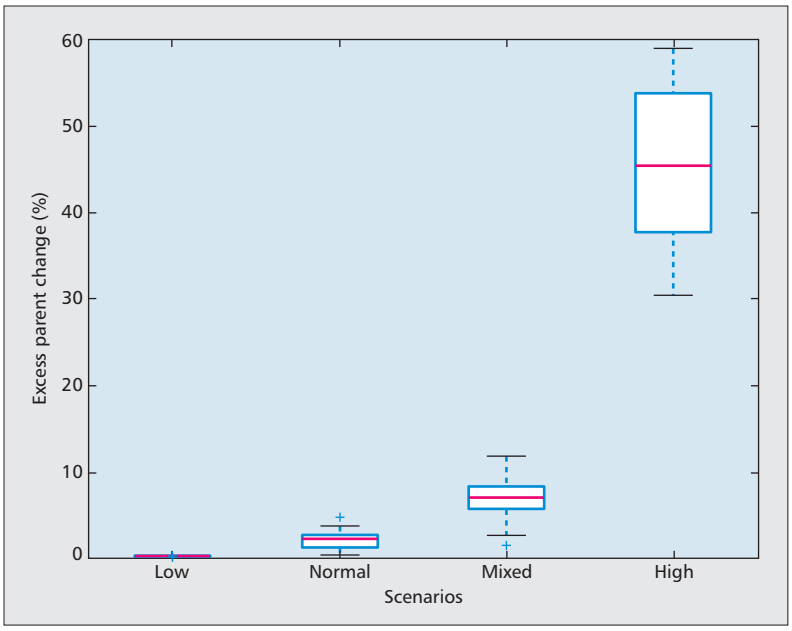

Figure 6. *Excess parent change under various interference scenarios.*

is not solely RPL's fault. Isolation between layers of the protocol stack is partly at fault. The performance of a network stack under any scenario depends on how each layer responds to the events taking place in the network. Although the lower layers of the stack might be able to guess the existence of interference, RPL is forced to treat the packet loss like any other packet loss. As a result the nodes spend a lot of energy getting few packets delivered.

The users care most about the performance of the complete system, not if the packet drops are due to RPL or the MAC layer or due to interference from WiFi. Research has shown that getting a network to work reliably under interference is challenging and requires coordination across the layers (more agile physical layer, less aggressive MAC, transport discriminating between different types of losses, moderation of data rates at the application) and types of devices.

Co-existence of different wireless technologies has been an area of active research for some time but in production system has been handled only implicitly, for example, by treating signals from overlapping communication by different radio technology as noise. To handle coexistence explicitly, there needs to be an architecture that allows coordination of devices through a common backchannel agreed upon by many parties in this ecosystem. This is easy to do in research.

Such coordinated response is much more difficult to achieve in practice because different standard bodies are responsible for standardizing different parts of the stack and types of radio technologies. IEEE defines most of the low level standards. IETF standardizes the network layer for the Internet. Then, there are alliances like ZigBee that extend all the way to the application layer. Recently, we have seen increasing coordination among the standards from different bodies. For example, the IETF 6LoWPAN standards are geared towards running IPv6 on top of IEEE 802.15.4 devices. ZigBee has recently adopted RPL as its routing layer.

Cross layer protocol research has shown that wider and more invasive interface between the PHY/MAC and network layers can improve the coordination between these layers to make the network more robust to interference and improve performance. Translating such cross layer designs to commercial products requires coordination between the IEEE, the IETF, and many other organizations. In the TCP/IP research, it is common to emphasize that certain enhancements to the protocol is achieved without changing packet format. If the cross-layer wireless network protocol research community embraced similar discipline while enhancing the interaction and visibility between PHY/MAC and network layer, the research results would be more likely to be adopted by the standardization bodies.

Conclusions

RPL is a recently standardized IETF routing protocol for low power and lossy networks. In this article, we share our findings from studying its performance under a variety of settings the network could encounter when it is deployed in practice. We found that it challenging to deliver data reliably even in environments that would be typical of smart homes or offices. Just the presence of wireless access points with normal traffic reduced packet delivery reliability to 92%. This is a scenario we expect to find at every home and many smart home and smart environments will have additional sources of interference. As we deploy massive number of devices, it is inevitable that many nodes will experience harsher wireless environments. For some applications, such as security, resource metering, and occupant tracking, poor performance as we observed in our experiments will be unacceptable. Research has shown that it is possible to deliver data reliably under interference. Protocols on which we run our smart homes should leverage such research.

Acknowledgments

This work was partly supported by a generous gift from Cisco. Thanks to Tom Cumpian and Babu Sundaram for providing access to the computer lab for measurements. Thanks to Prahal Arora for his help with performing experiment.

References

[1] E. T. Winter and E. P. Thubert, "Rpl: IPV6 Routing Protocol for Low Power and Lossy Networks," http://tools.ietf.org/html/ draft-ietf-roll-rpl-19, 2011.
[2] R. Xu *et al.*, "Muzi: Multi-Channel Zigbee Networks for Avoiding WiFi Interference," *Internet of Things (iThings/CPSCom), 2011 Int'l. Conf. and 4th Int'l. Conf. Cyber, Physical and Social Computing*, Oct. 2011, pp. 323–29.
[3] J. Huang *et al.*, "Beyond Co-Existence: Exploiting WiFi White Space for Zigbee Performance Assurance," *2010 18th IEEE Int'l. Conf. Network Protocols (ICNP)*, Oct. 2010, pp. 305–314.
[4] C.-J. M. Liang *et al.*, "Surviving Wi-Fi Interference in Low Power Zigbee Networks," *Proc. 8th ACM Conf. Embedded Networked Sensor Systems*, ser. SenSys '10, New York, NY, USA: ACM, 2010, pp. 309–22, available: http://doi.acm.org/10.1145/1869983.1870014.
[5] N. Accettura *et al.*, "Performance Analysis of the RPL Routing Protocol," *Mechatronics (ICM), 2011 IEEE Int'l. Conf.*, Apr. 2011, pp. 767–72.

[6] J. Tripathi, J. de Oliveira, and J. Vasseur, "A Performance Evaluation Study of RPL: Routing Protocol for Low Power and Lossy Networks," *2010 44th Annual Conf. Information Sciences and Systems (CISS),* Mar. 2010, pp. 1–6.
[7] O. Gaddour *et al.*, "Simulation and Performance Evaluation of Dag Construction with Rpl," *2012 2rd Int'l. Conf. Commun. and Networking (ComNet)*, Apr. 1–29, 2012, pp. 1–8.
[8] W. Xie et al., "A Performance Analysis of Point-to-Point Routing Along A Directed Acyclic Graph in Low Power and Lossy Networks," *2010 13th Int'l. Conf. Network-Based Information Systems (NBiS)*, Sept. 2010, pp. 111–16.
[9] T. Potsch *et al.*, "Performance Evaluation of COAP using RPL and LPL in Tinyos," *2012 5th Int'l. Conf. New Technologies, Mobility and Security (NTMS)*, May 2012, pp. 1–5.
[10] M. Kazandjieva *et al.*, "Powernet: A Magnifying Glass for Computing System Energy," *Proc. Stanford Energy & Feedback Workshop: End-Use Energy Reductions through Monitoring*, Feedback, and Behavior Modification, 2008.
[11] J. Hauer, "Tkn15. 4: An IEEE 802.15. 4 MAC Implementation for Tinyos 2," Telecommunication Networks Group, Technical University Berlin, TKN Technical Report Series TKN-08-003, 2009.
[12] J. Ko *et al.*, "Evaluating the Performance of RPL and 6lowpan in Tinyos," *Proc. Wksp. Extending the Internet to Low Power and Lossy Networks (IP+ SN 2011)*, Apr. 2011.

BIOGRAPHIES

DONG HAN (donny@cs.uh.edu) received his B.Sc.Eng. degree in computer science and technology in 2007 from Zhejiang University of Technology, China, and his M.S. degree in telecommunication engineering from the University of Sydney, Australia. He is enrolled as a Ph.D. student at the University of Houston, Texas. His current areas of research focuses on routing protocol in wireless sensor network, particularly fault-tolerance in CTP protocol, and user activity identification based on energy measurement study on desktop computers.

OMPRAKASH GNAWALI (gnawali@cs.uh.edu) is an assistant professor at the University of Houston. He was a postdoctoral scholar at Stanford University, got his Ph.D. from the University of Southern California, and received his Master's and Bachelor's degrees from the Massachusetts Institute of Technology. His research lies at the intersection of low-power wireless networks and embedded sensing systems.