Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 26, 2018
L. Feeney
Uppsala University
V. Fodor
KTH
May 25, 2018

Inter-network Coexistence in the Internet of Things
draft-feeney-t2trg-inter-network-03

Abstract

The breadth of IoT applications implies that there will be many diverse, administratively independent networks operating in the same physical location. In many cases, these networks will use unlicensed spectrum, due to its low cost and ease of deployment. However, this spectrum is becoming increasingly crowded. IoT networks will therefore be subject to wireless interference, both from similar networks and from networks that use the wireless channel in very different ways.

High-density, heterogeneous wireless environments present formidable challenges for network coexistence. The PHY and MAC layers are primarily responsible for managing how radios use the channel. But higher layer protocols are also a key factor in inter-network interaction. To date, there have been few performance studies of coexistence in future IoT operating environments, particularly with respect to protocol behavior and network-scale interactions.

This document describes key challenges for coexistence and highlights some recent research results that demonstrate the impact of protocol level interactions on network performance. It identifies both concrete and speculative opportunities for the IRTF T2TRG community. The former include developing and documenting best practices for performance evaluation and contributing IoT-related protocols being developed within IETF. The latter include speculative research into the design of high-layer protocols that allow networks to actively coordinate their access to the shared channel.

Table of Contents

1. Introduction

An IoT application is a set of wireless devices that act together to perform some sensing and control function. Most applications also have some connectivity to external resources, such as a mobile app or cloud-based service. In general, each application is deployed independently of any other applications that may be operating in the area and is a physically and administratively separate network.

An enormous range of IoT applications are expected to become pervasive in daily life. Networks will be installed in public spaces, businesses, and residences by a wide range of individual, commercial, and government actors. As a result, there will be many diverse, administratively independent networks operating in the same physical location. For example, a future home environment may include IoT applications for security, heating and cooling, elder care, air quality monitoring, personal health and fitness, smart home appliances, structural monitoring, lighting, utilities, and entertainment.

Many of these networks will use unlicensed spectrum due to low cost and simplicity of deployment for both the user and developer. In unlicensed spectrum, there is no authority that has a management relationship with (or even knows about) all of the potentially interfering networks that can be present in some location. This means that there is no entity that can coordinate networks' use of the shared wireless channel. Networks will therefore experience interference caused by transmissions from devices belonging to other networks.

The PHY and MAC layers have primary responsibility for ensuring that devices share the channel efficiently, while spectrum regulations limit devices' output power and overall channel utilization. But the MAC protocol can only explicitly coordinate devices within a single network. It provides only limited protection from other networks, some of which may have very different transmission footprints over time, spectrum or physical space.

Network coexistence is mainly evaluated in terms of PHY layer and radio hardware resilience to interference. This is generally based on analytic modeling of the probability of successful packet reception for varying SNIR conditions or on carefully controlled measurements of interacting RF waveforms. (See e.g. [NIST] for a discussion of relevant issues and [SKH11] for an example of such an analysis for IEEE 802.15.4g.)

Analytic modeling of network interactions at the MAC layer is much harder, because each network adapts its transmission parameters and

timing in response to the others. The presence of interfering networks is usually modeled as increasing the intensity of some statistical process representing noise or loss. Testbed tools, such as JamLab, have also been used to generate controlled interference. Other studies are based on simulation or testbed measurements of simple scenarios. The research literature contains a number of such studies, especially for IEEE 802.11 and IEEE 802.15.4. (See [SURVEY] and [SURVEY2] for an overview.)

In practice, currently deployed networks mostly rely on low IoT traffic loads and careful channel selection to achieve adequate performance. This may not be sustainable as rapid growth in IoT (and mobile data offloading) lead to increasing pressure on unlicensed spectrum. There are very few studies that evaluate complex, heterogeneous IoT interference scenarios, particularly with regard to protocol behavior and network-scale interactions. But as recent work [WETZ17] demonstrates, real world instances of IoT interference do occur and require considerable effort to diagnose.

This document explores key challenges for network coexistence in future IoT environments and highlights some recent research results ([FF16], [F3G15], [YTB17]). These suggest that protocol level interactions can significantly affect network performance, even in simple scenarios where the channel is not heavily loaded. Higher layer protocols will need to be aware of the potential impact of inter-network interference and avoid contributing to adverse interactions.

The community does not yet have a solid understanding of the reliability and effectiveness of IoT protocols in the presence of inter-network interference. In part, this is because the tools and techniques for performance evaluation of network coexistence scenarios are still immature. This document considers some of the challenges and requirements for both simulation and testbed approaches.

We also identify both concrete and speculative areas where T2TRG is well-positioned to contribute: The former includes the development of best practices for performance evaluation and informing the ongoing development of IoT-related protocols being developed within the IETF. The latter includes speculative research into the development of protocols that allow independent networks to actively coordinate their use of the shared wireless channel.

2. IoT interaction challenges

Widespread deployment of diverse IoT applications presents four main challenges: 1) scale 2) lack of a trust relationship between independently deployed networks 3) resource limitations, especially battery capacity 4) diversity of application requirements and channel utilization behavior.

2.1. Scale

As IoT becomes pervasive, there will be many independent networks operating in any given location. Devices will experience high levels of both homogeneous and heterogeneous radio interference.

Since networks use different kinds of radios and have different wireless coverage areas, their topologies will overlap with each other in complex ways. Interference will therefore involve not just individual wireless links, but also larger regions in the network and protocols operating at network scale.

Interaction scenarios will also be highly dynamic, with mobility and user activity leading to frequent changes in the set of interfering devices.

2.2. Independence

In unlicensed spectrum, there is no obvious basis for an administrative relationship between networks. Networks with overlapping wireless coverage may well have been deployed by at different times by unrelated actors. Nor is there any common authority that has an administrative relationship with all of the potentially interfering networks in any given location.

This means that there is no external entity that networks can trust to coordinate access to the shared channel. Devices within any one network will be able to authenticate themselves to each other and their own administrator (usually a non-expert user). But there is no way for them to authenticate themselves to each other - an IoT network may not have any meaningful external identity. Even if two networks can exchange this information, there is no obvious way for each to determine whether the other will participate appropriately with respect to some coexistence mechanism.

2.3. Resource limitations

IoT networks are severely resource constrained in many respects, including channel capacity, energy, hardware capabilities and cost.

The large number of devices sharing the wireless channel naturally limits the capacity available to each device. In addition, many devices use low bit-rate radios, which further reduces the communication capacity. (Note, however, that adverse interactions between networks can occur even in cases where the channel is only lightly used.)

For energy-harvesting and battery-powered devices, maximizing lifetime is essential. Protocol design is dominated by the need to minimize device activity and especially by the need to keep the energy-hungry radio turned off as much as possible, while still maintaining necessary connectivity. Even sensing the channel conditions is an extremely expensive operation. This limits networks' ability to observe and adapt to the behavior of their neighbors.

Finally, for many IoT applications, devices must be low cost and easily deployed and managed by non-expert users. They often have very limited memory and CPU resources. These factors constrain the design space and limit the complexity of proposed solutions.

2.4. Diversity

Even networks that use the same radio hardware and protocols will interfere with each other. But the diversity of IoT radios, protocols and applications creates additional challenges. Even characterizing the space of possible interactions may be challenging: Protocols can be anything from freely available, to consortia-driven standards such as ZigBee or WirelessHART, to completely proprietary.

This diversity is driven by the diversity of IoT applications. Applications will differ significantly in their devices' communication range and the overall network coverage area. They will vary in the number of devices and traffic load. They will have different requirements for latency and reliability. And they will use different energy sources and have different requirements on energy efficiency and lifetime. To meet these requirements, applications will use a wide variety of radios, protocols and network structures.

2.4.1. Radio and PHY

Different radio technologies divide the spectrum into channels differently: In the 2.4GHz unlicensed band, for example, IEEE 802.11 has up to 14 overlapping channels, while IEEE 802.15.4 and BluetoothLE have 16 and 40 non-overlapping ones. Radios also use a variety of modulation techniques at the PHY layer to define how data is encoded on the channel as RF energy.

This means that there are many different ways that RF energy is distributed over time and spectrum. As a result, it may not be possible for channel sensing mechanisms to reliably detect the presence of potentially interfering transmissions or identify the source of interference and packet loss.

Each PHY layer makes different tradeoffs between transmit power, communication range, bit-rate, bandwidth, energy consumption and resilience. In sub-GHz spectrum, for example, IEEE 802.15.4g/Wi-SUN (smart utility network) provides 50-200 kbps bit-rates with ranges of > 1000m. Very low power EnOcean devices provide similar bit-rates, but ranges of < 100m. By contrast, LoRa provides bit-rates of at most a few kbps, but can obtain 10km of range. Differences in bit-rate and frame size mean that packet transmit times can range from < 10 ms to > 200 ms. Radios operating in 2.4GHz, such as IEEE 802.15.4, IEEE 802.11 and Bluetooth, show similar diversity.

2.4.2. Network structures

Along with different kinds of radios, different kinds of network structures can be used to meet application requirements for density and coverage area. The most common structure is the star topology, where all devices communicate directly with a controller. Networks can also cover larger areas or achieve higher reliability by using multi-hop forwarding over various topologies, such as directed acyclic graphs, cluster trees, and meshes.

These structures affect how transmissions within a network are correlated with each other in time and space, such as forwarding a frame across a mesh. It can also affect interactions between networks, particularly networks whose radios have very different coverage areas. For example, a long-range device belonging to one network may be located in the midst of a mesh of short-range devices belonging to another network.

2.4.3. Protocols

The MAC layer defines how senders coordinate their transmissions within a network. Like the PHY layer, different MAC layers create different distributions of RF energy in time and (for channel hopping protocols) spectrum.

CSMA-based (channel sensing and backoff) protocols can provide some protection from external transmissions, since they defer to any ongoing transmission that they detect. Conflicts due to hidden terminals can occur even within a single network, but differences between radio technologies and network structures may exacerbate the problem. In addition, MAC timing parameters, such as backoff times,

are generally proportional to bit-rate and frame transmit times. Timing incompatibilities between interfering senders can reduce the effectiveness of backoff and retransmissions in heterogeneous environments.

TDMA-based (transmission schedule) protocols can be more efficient in their use of the channel and energy than CSMA protocols. But because the networks define their slot structure and transmission schedules independently, they may allocate transmission slots that conflict with each other. Since senders rely on their assigned schedule, such conflicts can be costly.

Minimizing energy consumption is often the absolute priority for IoT design. It is necessary to keep radio turned off as much as possible, while still ensuring connectivity. As with MAC protocols (with which they are sometimes integrated), there are a variety of approaches. With synchronous methods, devices wake up according to a schedule that ensures that senders and receivers are awake at the same time (as in IEEE 802.15.4 beacon-enabled PANs or TSCH). Asynchronous methods allow devices to coordinate their wake up schedules on-demand (as in ContikiMAC).

Coordinating the duty cycles of a sender and receiver imposes strict timing constraints on radio operations. As with the PHY and MAC, each power save protocol creates its own distribution of RF energy over time. Depending on application requirements and tradeoffs for latency and battery lifetime, duty cycles could be on timescale of < 1s to > 1000s.

Many IoT networks use IP(v6), but there is also considerable diversity in higher layer protocols, both open and proprietary. Routing protocols make different tradeoffs between latency, reliability, energy efficiency and overhead, depending on the application requirements. The operation of the routing protocol also affects the distribution of RF energy in physical space, as frames are forwarded toward a root or across a mesh. The routing protocol may also react to the presence of interference by attempting to re-route its traffic.

Higher layer protocols largely abstract away from the behavior of individual wireless links. They use a variety of mechanisms to maintain communication performance under conditions of loss and delay, including retransmissions, multi-path communication, and application-specific adaptations.

Finally, the variety of transport, transfer and application protocols used in IoT networks reflects the diversity of use cases: The RESTful model is central for IoT applications based on web services

[I-D.keranen-t2trg-rest-iot]. Wireless sensing applications often use in-network data processing and aggregation to reduce their communication load. Industrial IoT applications emphasize low latency and reliability. Wide-area IoT/SUN networks collect small amounts of data from a very large number of devices. As a result, applications may have very different priorities with respect to packet loss, delay, and energy consumption.

3. Interaction behaviors

All elements of network functionality - MAC, power saving, topology and routing, congestion control, data transfer, application - contribute patterns of channel utilization over time, frequency, and physical space. At the same time, protocols adapt their behavior in response to channel conditions; relying on channel sensing and frame errors at low layers and on loss and delay at higher layers. Inter-network interaction therefore occurs on multiple time- and spatial-scales and involves all layers of the protocol stack.

Motivating scenarios include:

o How will sub-GHz LPWAN networks such as LoRa and SigFox, whose base stations cover wide areas, interact with multiple shorter-range networks using IEEE 802.15.4g/WiSUN, Z-Wave, or EnOcean radios?

o What happens if two or more independent networks using 6LoWPAN+RPL+CoAP are operating in the same room? Or two 6TiSCH networks, each using a different scheduling function? What if an a beacon-enabled PAN interacts with a ZigBee- or ContikiMAC- or Thread-based network? What if people wearing BluetoothLE-based body-area networks are also moving around in the area? Especially in a WiFi heavy environment, the value of channel hopping for interference mitigation may be limited.

o More generally, can networks using protocols optimized for different metrics (e.g. latency vs battery lifetime) operate effectively in the same location?

To date, there have been very few studies that examine network performance under realistic - dense, heterogeneous, dynamic - interference scenarios. Some existing observations and results are noted here.

3.1. WiFi

Interference between WiFi networks is a long-standing problem, particularly in dense residential and urban areas, where there are many independently deployed networks and large amounts of traffic.

To some extent, this has been mitigated by expansion into 5GHz unlicensed spectrum and by major improvements in WiFi, including higher bit-rates and directional transmission (beamforming). The WiFi environment also has some properties that are helpful for coexistence: WiFi networks are largely homogeneous, consisting of an AP and associated devices that communicate directly with their AP. WiFi also uses a CSMA-based MAC, which means that senders inherently defer to any ongoing WiFi transmission, regardless of its source. And the dominant application is media streaming, which is supported by adaptive mechanisms everywhere from the server to the user application.

However, WiFi performance may come under increasing pressure, due not only to the increasing number of IoT networks, but also to the forthcoming deployment of LTE traffic into 5GHz unlicensed spectrum.

3.2. IEEE 802.15.4

A common scenario in 2.4GHz spectrum will involve high-power, high-traffic WiFi networks impacting networks based on low power, low bit-rate radios, such as IEEE 802.15.4.

Practical existing solutions are mostly based on IEEE 802.15.4 devices identifying and using the least interfered channels, either statically or by channel hopping. But in areas where there is a lot of WiFi traffic, there may be very few such channels. WiFi conventionally uses non-overlapping WiFi channels 1, 6, and 11, leaving just three minimally interfered IEEE 802.15.4 channels. As a result, low power IoT networks operating in these areas may be crowded into a small number of "good" channels. These may come under increasing pressure as IoT deployment increases.

3.3. Recent results in IoT networks

Recent research suggests that protocol level interactions can lead to severe performance degradation, even when the channel is not heavily loaded. While these studies focus on various IEEE 802.15.4 MAC layers, the results suggest broader implications for protocol design.

[F3G15] and [FF16] show that IEEE 802.15.4 beacon-enabled PANs can experience episodes of severe disruption due to protocol level interactions. This includes behaviors such as short-term

oscillations in throughput and extended periods of disconnectivity - even when the channel itself is only lightly loaded. Similarly, [YTB17] shows that interfering IEEE 802.15.4 6TiSCH-based networks experience packet loss and so-called blackout periods, as well as increased energy consumption.

These behaviors appear to be due to a combination of timing rigidities in the MAC protocol, periodicity in the radio duty cycle, and clock drift between networks. Battery constraints force devices to spend most of their time with their radios turned off. Senders and receivers therefore need some way to coordinate their radio wake up times so that they can exchange packets. These mechanisms often depend heavily on careful timing of radio operations, instead of (or in addition to) explicit control traffic. This timing dependence can make networks more sensitive to disruption than might be expected from just considering overall channel utilization and collision probabilities. Periodicity can exacerbate these effects. In addition, clock drift results in networks' synchronizing and desynchronizing with each other. This can result in interaction effects at timescales on the orders of minutes or even days. Generalizing these observations suggests that it will be necessary to reconsider tradeoffs between energy consumption and resilience.

3.4. Higher layer protocols

To date, there have been few studies that address the performance of high layer protocols, such as routing or data transfer, in network coexistence. Certainly, extended outages at the link layer will affect their operation and there is a risk that higher layer protocols' reaction will exacerbate the impact of interference. Conversely, it is possible that higher layer protocols may act to mitigate the impact of interference, e.g. through congestion avoidance.

4. Network coexistence in the IRTF/IETF context

The research literature contains a variety of proposals for improving protocol performance in the presence of interference (see [SURVEY], [SURVEY2] for an overview). In many cases, they assume rather narrowly defined interaction scenarios and none seem to have been deployed in practice.

Network coexistence in realistic IoT environments remains an open issue, particularly with respect to protocol and network-scale interactions. T2TRG is well-positioned to contribute to addressing it by:

- o Developing and advocating best practices for performance evaluation, focusing on realistic future wireless environments.

- o Contributing to the ongoing development of IoT-related IETF protocols, so that they are as resilient as possible to inter-network interference.

- o Supporting speculative research into the possibility of higher layer protocols for active coordination between networks sharing unlicensed spectrum.

4.1. Performance evaluation and protocol design

Performance evaluation of IoT protocols should take into account their behavior in the presence of many diverse, administratively independent networks operating in the same spectrum. To date, there have been few studies that fully reflect this aspect of the future IoT operating environment. This suggests that the community does not yet have a complete understanding of effectiveness and reliability of IoT protocols.

Given the community's limited experience with such evaluation, it is unsurprising that there are not yet clear principles for designing experiments that can provide meaningful results. Experiments must reflect a realistic interference environment and capture behaviors caused by interactions within the protocol stack, within a network, and between networks - while still being both manageable and informative for the the user. Best practices for designing such experiments have not been established and existing simulation and testbed tools have significant limitations.

Protocol-oriented network simulators (e.g. ns-2/3, OMNeT++, OPNET) enable performance evaluation at scale: It is straightforward to simulate an extremely large number of scenarios behavior over a long period. Simulation also provides complete control and visibility into the operation of the simulated system. However, these advantages come at the cost of reduced fidelity, especially for wireless propagation and reception. Modeling of interference between different kinds of radios is particularly lacking.

By contrast, testbeds provide ground-truth about network performance in a specific scenario. There are a number of open WSN/IoT testbeds (e.g. [FINTEROP], [FITIOT]) that provide access to various collections of hardware. However, the community has had little experience using them for evaluating coexistence scenarios.

There are three main challenges: One is the logistics of deploying long-running experiments involving multiple applications and many

devices. Another practical challenge is instrumenting and collecting data from the entire protocol stack and correlating the results across networks, especially with resource-constrained devices. This functionality is essential for obtaining data that allows users to reason about the observed performance. Finally, there is a deeper challenge in defining experiments that allow the user to systematically explore the space of possible interactions, despite the complexity and variability of the inter-network interference environment.

In this context, T2TRG can contribute to the development of and advocacy for best practices for performance evaluation. The results of such studies can inform ongoing protocol development. This includes protocols being developed in the IETF 6lo, 6TiSCH (especially 6top), LPWAN, LWIG, ROLL and CoRe Working Groups. (It is, of course, also necessary to take into account interactions with protocols from other open and proprietary sources.)

4.2. Adaptive mitigation strategies

Network coexistence is likely to rely heavily on improving resilience to interference in the MAC layer, which is ultimately responsible for determining when a sender transmits.

But a MAC protocol cannot explicitly coordinate with devices in other networks; it may not even be able to identify what kinds of networks are sharing the channel, much less exchange (authenticated) control traffic. The MAC layer must instead adapt to the presence of other networks based on channel sensing and frame loss. This is a significant challenge in complex interference environments, especially for battery-powered devices, which must avoid the high energy cost of listening to the channel as much as possible. While the MAC layer and power saving protocols are themselves largely outside IETF scope, these topics are relevant to the work of IETF WG's such as 6lo, 6TiSCH, LPWAN and LWIG.

Like the MAC layer, higher layer protocols also adapt their behavior, using packet loss and delay. But complex interactions such as those described above can lead to disruptions that are difficult for higher layer protocols to predict or adapt to in an effective way. It is therefore important to ensure that protocol behaviors, such as route selection, congestion control or keep-alive mechanisms, contribute to (or at least do not hurt) resilience to inter-network interference. These topics are particularly relevant to IETF protocols such as RPL and CoAP.

4.3. Active mitigation strategies

More speculatively, there may be opportunities for higher layer protocols to actively participate in interference mitigation, by sharing information about their operation and even by explicit coordination between networks.

When two networks use the same PHY layer, it is possible for frames transmitted by devices in one network to be successfully received by devices in other networks. These frames are usually discarded immediately, since they fail a MAC layer authentication check. But if they are not discarded (and are not encrypted), the networks can observe each others' control traffic or even explicitly exchange information. Such a mechanism could allow them to announce their expected channel utilization patterns, for example. MAC layer or even IPv6 frames could be used for this purpose.

Alternatively, many IoT applications have some administrative component that is connected to the Internet infrastructure, such as mobile app-based user interface or cloud-based data collection. Even limited connectivity opens possibilities for making use of a rich array of resources. For example, this may be a way to provide access to additional computing power or to allow networks make use of external services with which they have an administrative relationship. This might enable a coordination mechanism based on negotiation via some trusted cloud-based service.

The inspiration here is from several different approaches: Cognitive radio solutions where secondary users obtain information about activity of primary users from trusted sources; Citizens Broadband Radio Service (CBRS) and its spectrum allocation service; and research into distributed coordination services e.g. [SEMCK14]. However, all of these approaches rely on either strict spectrum regulation or a strong assumption of compatibility and cooperative behavior among networks.

Even more speculatively, a secure distributed ledger could be used to allow networks to announce themselves in a location, to provide information about their channel utilization, and to obtain information about co-located networks. Such a ledger could further act as a reputation management system or as a resource broker. This is potentially related to distributed infrastructure work in the IRTF DINRG.

However, these are very much an open research area and there are substantial challenges in developing such mechanisms:

1) There is an enormous diversity of radios, channel access methods and utilization patterns that might need to be described. It is not clear what information should be signaled or what actions a receiver should take in response.

2) Battery lifetime, channel capacity, and device CPU and memory resources continue to be significant limitations. In particular, the radio duty cycle is highly constrained, limiting both sensing and communication.

3) Any cooperative mechanism must operate effectively in the absence of any administrative or trust relationship between networks. Alternatively, there must be some way to establish an appropriate level of trust. This presents a significant challenge to the practical implementation of cooperative mechanisms proposed in the literature. (See Security Considerations below.)

4) The privacy implications of networks sharing information about their activity must be carefully considered. (See Security Considerations below.)

Despite the challenges, this topic seems particularly amenable to standards and interoperability-oriented approaches enabled by IRTF T2TRG. There may be synergy with IRTF T2TRG work in IoT semantic interoperability: Can IoT networks describe not only the 'things' they connect, but also themselves? In addition, the IRTF DIN research group is active in the area of secure distributed Internet infrastructure.

4.4. Role of Spectrum Regulation

Network coexistence is ultimately a problem of spectrum regulation. Regulation of unlicensed spectrum has historically focused on output power and overall spectrum utilization. For example, in 868 MHz spectrum, LoRa relies on transmit duty cycle (DC) limits (which range from 0.1% to 1%, depending on sub-band) to ensure efficient channel utilization.

In some cases, listen-before-talk (LBT) has been mandated for unlicensed bands, including (optionally) 868MHz. This results in a more complex regulatory structures, due to the need to specify detection thresholds, listening intervals, and backoff behaviors. The regulations specify minimum requirements, rather than a mechanism that is common to all networks. This can lead to networks with different backoff behaviors sharing a channel. Issues of compatibility and fairness between various LBT strategies are an active topic of study, notably with regard to WiFi and LTE coexistence in 5GHz spectrum (e.g. [KYK16]).

The IETF community has a strong interest in ensuring that spectrum regulation not only enables efficient use of unlicensed spectrum for IoT applications, but also avoids overly prescriptive mandates that constrain diversity and innovation.

5. Security Considerations

An overview of security challenges in IoT environments is given in [I-D.irtf-t2trg-iot-seccons]. The current document focuses on coexistence between independently administrated networks operating in the same location. The biggest security challenge for managing network interactions is that such networks do not necessarily have any basis for a trust relationship.

Regulations concerning unlicensed spectrum only control radio behaviors such as transmit power and overall channel utilization. Regulations do not mandate the use of any specific protocol. It is therefore not possible to externally enforce that networks participate in some specific coexistence protocol (as long as they otherwise comply with regulations).

Most wireless protocols adapt their behavior to channel conditions to some extent, such as contention backoff, channel blacklisting, or re-routing. But the more a network changes its behavior in response to small amounts of information from an untrusted source, the more leverage an attacker has to disrupt it. Similarly, the more information about its future behavior a network provides to an untrusted destination, the easier it is for an attacker to disrupt it. The risk is further exacerbated in energy-constrained networks, because a device may be forced to spend energy unnecessarily. In addition, the high energy cost of listening to the channel makes it expensive to build trust by observing the behavior of other networks.

Any proposed solution will therefore need to be resilient to the possibility of incompatible, oblivious, selfish, or even hostile networks when designing a coexistence mechanism. This is especially true for methods in which two networks actively coordinate their use of the shared channel. At a minimum, participating in information exchange should not substantially increase vulnerability to disruption in the case of a malicious (or merely incompatible) actor.

In addition, networks that try to be friendly toward each other may disclose substantial information about their operation. There are privacy issues associated with IoT networks making such information visible, because of their close coupling with human activity. Particularly for health-related applications, even being able to identify the type of application or its level of activity may reveal sensitive data. Ideally, it should be possible for a network to both

obfuscate its communication patterns (if needed) and act cooperatively.

One maxim that may be useful in designing the set of information that a network discloses as a matter of course with the intention of facilitating coexistence is that the information disclosed should not provide more insight than that information an attacker might have gained by simply observing the network for a while. But note that simply disclosing that information in an accessible way still changes the economy of surveillance -- the objective is that it also changes the economy of coexistence, and these effects need to be carefully weighed against each other.

6. Conclusion

The future IoT operating environment will contain many diverse, administratively independent networks sharing unlicensed spectrum. Ensuring network coexistence is essential for avoiding the "tragedy of the commons" and enabling practical deployment of IoT solutions.

The community currently lacks a good understanding of the impact of inter-network interactions, particularly with regard to protocol behavior and network-scale interactions. However, recent results for both IEEE 802.15.4 PANs and 6TiSCH + RPL networks suggest that inter-network interactions can lead to episodes of significant disruption, even when the channel itself is not overloaded. More research is needed into both the causes of adverse interactions and ways to mitigate them, particularly with regard to the role of higher layer protocols.

Network coexistence is and will continue to be largely driven by spectrum regulation and the PHY and MAC layers. However, this issue are also relevant to the work of IETF Working Groups, such as 6lo, 6TiSCH, LPWAN, ROLL, CoRE, and LWIG. We identify three areas where T2TRG can play a significant role:

o Performance evaluation should reflect that the IoT wireless environment will contain diverse interfering networks. Tools and techniques for investigating inter-network interaction are still immature. The community could benefit substantially from the development and documentation of best practices in this area.

o The results of such performance evaluation can assist IETF Working Groups in improving the resilience of IoT-related protocols.

o There may also be a role for novel network coexistence mechanisms based on information sharing or explicit coordination between networks. This is a speculative research topic that seems

particularly amenable to standards and interoperability oriented approaches. However, there are substantial challenges.

7. Informative References

[F3G15] Feeney, L., Frey, M., Fodor, V., and M. Gunes, "Modes of inter-network interaction in beacon-enabled IEEE 802.15.4 networks", 2015 14th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), DOI 10.1109/medhocnet.2015.7173294, June 2015.

[FF16] Feeney, L. and V. Fodor, "Reliability in co-located 802.15.4 personal area networks", Proceedings of the 6th ACM International Workshop on Pervasive Wireless Healthcare - MobiHealth '16, DOI 10.1145/2944921.2944923, 2016.

[FINTEROP] Kim, E. and S. Ziegler, "Towards an open framework of online interoperability and performance tests for the Internet of Things", 2017 Global Internet of Things Summit (GIoTS), DOI 10.1109/giots.2017.8016248, June 2017.

[FITIOT] Adjih, C., Baccelli, E., Fleury, E., Harter, G., Mitton, N., Noel, T., Pissard-Gibollet, R., Saint-Marcel, F., Schreiner, G., Vandaele, J., and T. Watteyne, "FIT IoT-LAB: A large scale open experimental IoT testbed", 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), DOI 10.1109/wf-iot.2015.7389098, December 2015.

[I-D.irtf-t2trg-iot-seccons] Garcia-Morchon, O., Kumar, S., and M. Sethi, "State-of-the-Art and Challenges for the Internet of Things Security", draft-irtf-t2trg-iot-seccons-15 (work in progress), May 2018.

[I-D.keranen-t2trg-rest-iot] Keranen, A., Kovatsch, M., and K. Hartke, "RESTful Design for Internet of Things Systems", draft-keranen-t2trg-rest-iot-05 (work in progress), September 2017.

[KYK16] Kim, C., Yang, C., and C. Kang, "Adaptive Listen-Before-Talk (LBT) scheme for LTE and Wi-Fi systems coexisting in unlicensed band", 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), DOI 10.1109/ccnc.2016.7444845, January 2016.

[NIST] Koepke, G., Young, W., Ladbury, J., and J. Coder, "Interference and Coexistence of Wireless Systems in Critical Infrastructure", National Institute of Standards and Technology report, DOI 10.6028/nist.tn.1885, July 2015.

[SEMCK14] Skjegstad, M., Ellingsater, B., Maseng, T., Crowcroft, J., and O. Kure, "Large-scale distributed Internet-based discovery mechanism for dynamic spectrum allocation", 2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN), DOI 10.1109/dyspan.2014.6817824, April 2014.

[SKH11] Sum, C., Kojima, F., and H. Harada, "Coexistence of homogeneous and heterogeneous systems for IEEE 802.15.4g smart utility networks", 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), DOI 10.1109/dyspan.2011.5936241, May 2011.

[SURVEY] Han, Y., Ekici, E., Kremo, H., and O. Altintas, "Spectrum sharing methods for the coexistence of multiple RF systems: A survey", Ad Hoc Networks Vol. 53, pp. 53-78, DOI 10.1016/j.adhoc.2016.09.009, December 2016.

[SURVEY2] Baccour, N., Puccinelli, D., Voigt, T., Koubaa, A., Noda, C., Fotouhi, H., Alves, M., Youssef, H., Zuniga, M., Boano, C., and K. Roemer, "External Radio Interference", SpringerBriefs in Electrical and Computer Engineering pp. 21-63, DOI 10.1007/978-3-319-00774-8_2, 2013.

[TCG316] Tinnirello, I., Croce, D., Galioto, N., Garlisi, D., and F. Giuliano, "Cross-Technology WiFi/ZigBee Communications: Dealing With Channel Insertions and Deletions", IEEE Communications Letters Vol. 20, pp. 2300-2303, DOI 10.1109/lcomm.2016.2603978, November 2016.

[WETZ17] Wetzker, U., Splitt, I., Zimmerling, M., Boano, C., and K. Romer, "Troubleshooting Wireless Coexistence Problems in the Industrial Internet of Things", 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), DOI 10.1109/cse-euc-dcabes.2016.167, August 2016.

[YTB17] Ben Yaala, S., Theoleyre, F., and R. Bouallegue, "Cooperative resynchronization to improve the reliability of colocated IEEE 802.15.4 -TSCH networks in dense deployments", Ad Hoc Networks Vol. 64, pp. 112-126, DOI 10.1016/j.adhoc.2017.07.002, September 2017.

Acknowledgements

The authors would like to thank Michael Frey, Charalampos Orfanidis, Martin Jacobsson, and Per Gunningberg for their valuable collaboration in simulation and measurement studies of inter-network interference. We would also like to thank Carsten Bormann for his support and encouragement in preparing this document, particularly the discussion of security considerations. David Oran's detailed comments on the text are also much appreciated.

Authors' Addresses

Laura Marie Feeney
Uppsala University
Box 337
Uppsala SE-751 05
Sweden

Email: lmfeeney@it.uu.se

Viktoria Fodor
KTH
Osquldas vaeg 10
Stockholm SE-100 44
Sweden

Email: vjfodor@kth.se