Avoiding an IoT ’Tragedy of the Commons’

Laura Marie Feeney
Uppsala University, Sweden
lmfeeney@it.uu.se

Per Gunningberg
Uppsala University, Sweden
perg@it.uu.se

ABSTRACT

The large number and wide diversity of IoT networks operating in unlicensed spectrum will create a complex and challenging interference environment. To avoid a ’tragedy of the commons’, networks may need to more explicitly coordinate their use of the shared channel.

CCS CONCEPTS

• **Networks** → **Network protocol design**;

1 INTRODUCTION

Since the early 2000’s, the spread of WiFi has led to speculation about a “tragedy of the commons”[8], in which networks would become unusable because they could not efficiently share the increasingly crowded wireless channel. This outcome was largely avoided thanks to major improvements in the radio and protocols, as well as expansion into 5GHz spectrum.

The growth of IoT, BAN, and LPWAN applications means that there will be a large number networks operating in a given location. Many of them will use unlicensed spectrum, due to its low cost and ease of deployment. These networks will be extremely diverse, using different radios, protocols, and network structures to meet a wide range of application requirements for coverage, throughput, latency, reliability, and power consumption. Because these networks are deployed by many different actors, they do not have any administrative relationship with each other or with a common authority.

These factors will contribute to a complex and challenging inter-network interference environment, leading to renewed concern. Improvements to existing IoT radios and protocols will undoubtedly once again play an important role in avoiding a new “tragedy”. Here, we present a complementary solution that allows networks to actively coordinate their use of the shared channel, despite the lack of trust between them.

2 NETWORK INTERACTION

All parts of the protocol stack – radio, PHY, MAC, power saving, topology and routing, congestion control, application – create patterns of channel utilization over time, frequency, and physical space. At the same time, protocols adapt their communication behavior in response to channel conditions; relying on channel sensing and frame errors at low layers and on loss and delay at higher layers.

But these mechanisms are most effective at coordinating the activity of devices within a single network. They can provide only limited coexistence with other unknown networks, which are also using and adapting to channel conditions, possibly in ways that lead to adverse interactions. Devices’ ability to observe the behavior of other networks may be severely limited, due to the need to minimize idle listening at the energy-hungry radio.

Recent results suggst that protocol-level and network-scale interactions can have a significant effect on IoT performance. Interfering IEEE 802.15.4 PANs [3, 5, 7] and 6TiSCH+RPL [9] networks are seen to suffer intermittent episodes of severe disruption, even when the channel is only lightly loaded. This includes behaviors such as rapid oscillations in throughput and extend communication blackouts. The underlying cause is a combination of timing rigidities in the power saving mechanisms, periodic behaviors, and clock drift between networks – highlighting a tradeoff between energy and resillience.

Network performance in plausible future IoT interference scenarios is not yet well understood and that there may be a real risk for an IoT “tragedy of the commons”. This has been a topic of recent discussion in the IRTF Thing-to-Thing research group (T2TRG) [4].

3 NETWORK COEXISTENCE

Improving protocols’ ability to adapt to complex interference environments will surely be an active area of investigation. But the challenges remain formidable, especially for devices with limited hardware and energy resources operating in very dense, dynamic, heterogeneous wireless environments.

MobiSys ’18, June 10–15, 2018, Munich, Germany

ACM ISBN 978-1-4503-5720-3/18/06.
https://doi.org/10.1145/3210240.3223572

Explicit information about the channel activity of other networks can allow networks to more actively coordinate their use of the channel. Proposed mechanisms include observing (unencrypted) control frames, explicit announcements of channel utilization, and even active negotiation of channel access (recent surveys include [6] and [1].) But such coordination implicitly depends on mutual awareness and an existing trust relationship between networks. This is not found in many IoT scenarios, where administratively independent networks may be incompatible, oblivious, selfish, or even hostile.

An effective solution therefore requires two things: a way for networks to exchange information on the wireless channel and a way for them to safely participate in some coordination scheme. We envision a complementary approach that leverages IoT networks' connectivity to resources in the the Internet infrastructure to establish their bona fides.

3.1 Inter-network communication

To coordinate, networks must be able to exchange at least a small amount of information over the wireless channel. When networks use the same radio/PHY and operate on the same channel, this is trivial. Radios receive frames from nearby senders, regardless of what network they belong to. Such frames are usually discarded by MAC layer authentication. But as long as the payload is not encrypted, it can be decoded by any receiver.

Networks that use different radios may also be able to establish direct connectivity. It is surprisingly feasible to exchange bits between networks that use quite different radios. Cross-technology communication (CTC) (e.g. [2, 10]) has been demonstrated between various combinations of WiFi, IEEE 802.15.4, and BLE, with rates of 100's to 1000's of bps. It should be noted, however, that coordinating CTC between interfering networks itself an open coexistence problem: How does a network know when to send or to listen for CTC "frames"?

3.2 Establishing trust

In unlicensed spectrum, networks do not have any administrative relationship with each other or with a common authority. This means that there is no obvious basis for a trust relationship between them: The networks are unknown to each other, do not share cryptographic keys, and may not even have any meaningful external identity.

There are considerable risks to both sender and receiver in exchanging information with unknown and untrusted networks. By describing its intended channel utilization, a sender risks making it trivially easy for a hostile receiver to jam it. Similarly, a receiver cannot safely act on information from the sender. By altering its behavior – especially if it spends energy – in response to a small amount of information, a receiver is providing considerable leverage to a potential attacker.

For such coordination mechanisms to be viable, networks must therefore establish some trust relationship. Especially in battery-powered networks which must minimize radio use, it may be infeasible for trust to be established based on observations of other networks' behavior. Some more structured method is needed.

Many IoT applications do have an administrative relationship with and (possibly limited) connectivity to some entity in the Internet infrastructure, such as a mobile app-based UI or cloud-based service. Establishing a trust relationship can thus be based on untrusted information exchanged over the shared wireless channel, combined with trusted resources of the Internet infrastructure.

Information exchanged on the wireless channel allows interfering networks to demonstrate that they are colocated and indicate their connection to the Internet infrastructure. This might be a vendor or service provider, ie. an entity that has a real-world identity and reputation. If each vendor agrees that the other is well-behaved – perhaps simply via blacklist – it encourages and assists its network to cooperate. The rich resources of the Internet can also be used to facilitate more complex coordination and trust mechanisms.

An even more speculative possibility is for networks to maintain a secure distributed ledger. Networks could to use their Internet presence to announce themselves in a location, to provide information about their channel utilization and to obtain information about other colocated networks. The ledger could act as reputation management system or as a resource broker.

4 CONCLUSION

In closing, we note that network co-existence is fundamentally an issue of spectrum regulation. Regulation of unlicensed spectrum has historically focused on power and overall spectrum utilization, rather than mandating any specific protocol. This flexibility has contributed to successful innovation and it remains important to avoid overly prescriptive regulation.

To avert an IoT 'tragedy of the commons', it is necessary not only to improve protocols' ability to adapt to complex interference environments, but also to provide ways for networks to safely coordinate their use of the shared channel. We have envisioned one such approach. Because these mechanisms cannot (and should not) be mandated, they will need to perform well to create norms and incentives that lead to their widespread adoption.

REFERENCES

[1] Nouha Baccour, Daniele Puccinelli, Thiemo Voigt, Anis Koubaa, Claro Noda, Hossein Fotouhi, Mario Alves, Habib Youssef, Marco Antonio Zuniga, Carlo Alberto Boano, et al. 2013. External radio interference. In *Radio Link Quality Estimation in Low-Power Wireless Networks*. Springer, 21–63.

[2] Daniele Croce, Natale Galioto, Domenico Garlisi, Fabrizio Giuliano, and Ilenia Tinnirello. 2017. An Inter-Technology Communication Scheme for WiFi/ZigBee Coexisting Networks. In *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*. 305–310.

[3] Laura Marie Feeney and Viktoria Fodor. 2016. Reliability in co-located IEEE 802.15. 4 personal area networks. In *Proceedings of the 6th ACM International Workshop on Pervasive Wireless Healthcare*. 5–10.

[4] Laura Marie Feeney and Viktoria Fodor. 2017. *Inter-network Coexistence in the Internet of Things*. Internet-Draft draft-feeney-t2trg-inter-network-01. IETF Secretariat.

[5] Laura Marie Feeney, Michael Frey, Viktoria Fodor, and Mesut Gunes. 2015. Modes of inter-network interaction in beacon-enabled IEEE 802.15. 4 networks. In *14th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*. 1–8.

[6] You Han, Eylem Ekici, Haris Kremo, and Onur Altintas. 2016. Spectrum sharing methods for the coexistence of multiple RF systems: A survey. *Ad Hoc Networks* 53 (2016), 53–78.

[7] Noorsalwati Nordin and Falko Dressler. 2012. Effects and implications of beacon collisions in co-located IEEE 802.15. 4 networks. In *Vehicular Technology Conference (VTC Fall)*. 1–5.

[8] Douglas Sicker, Christian Doerr, Dirk Grunwald, Eric Anderson, Brita Munsinger, and Anmol Sheth. 2006. Examining the wireless commons. (2006).

[9] Sahar Ben Yaala, Fabrice Théoleyre, and Ridha Bouallegue. 2017. Cooperative resynchronization to improve the reliability of colocated IEEE 802.15. 4-TSCH networks in dense deployments. *Ad Hoc Networks* 64 (2017), 112–126.

[10] Zhimeng Yin, Wenchao Jiang, Song Min Kim, and Tian He. 2017. C-morse: Cross-technology communication with transparent morse coding. In *IEEE Conference on Computer Communications (Infocom)*. 1–9.

ACKNOWLEDGMENTS

The authors would like to thank Viktoria Fodor at KTH and participants in the IRTF T2TRG and DINRG research groups for valuable comments and discussion.