Competition: Using DeCoT+ to Collect Data under Interference

Xiaoyuan Ma[1,3], Peilin Zhang[4], Ye Liu[5], Xin Li[1,2], Weisheng Tang[1,3], Pei Tian[1,3], Jianming Wei[1], Lei Shu[5], Oliver Theel[4]
1. Shanghai Advanced Research Institute, Chinese Academy of Sciences, China
2. ShanghaiTech University, School of Information Science & Technology, China
3. University of Chinese Academy of Sciences, China
4. Carl von Ossietzky University of Oldenburg, Germany
5. Nanjing Agricultural University, China
{maxy, lixin01, tangws, wjm, tianpei2018}@sari.ac.cn
{peilin.zhang, theel}@informatik.uni-oldenburg.de
{yeliu, lei.shu}@njau.edu.cn

Abstract

Toward the scenario of data collection in EWSN 2019 Dependability Competition, we base our design on the efficient concurrent transmission. Moreover, there are two critical mechanisms to guarantee the dependability of the protocol, i.e., the channel-hopping and the network initiation. The **De**pendable **Co**ncurrent **T**ransmission-based protocol (DeCoT) performs effectively in the past competitions where an event was represented as a tiny payload.

Variable lengths of payloads and dynamic traffic loads are new challenges appearing in the EWSN 2019 Dependability Competition. A **Con**sistency Strategy and a **Ne**twork **C**oding (ConNec) are functional to overcome the challenges. Therefore, we propose DeCoT+, DeCoT with ConNeC, that oughts to work effectively in a dynamic (heavy or light) traffic loads under interference. Besides, the network coding strategy could improve the reliability of the network, where nodes communicate with long packets, e.g., 64 bytes.

1 Introduction

In 2017, we proposed OF∂COIN [7] based on the concurrent transmission (CT) to propagate simple events from one source to one destination dependably under interference. In 2018, an enhanced OF∂COIN (eOF∂COIN) [9], supporting many-to-all communications, was proposed to monitor multiple concurrent events under adverse conditions. Both protocols achieved high reliability under interference. Specifically, Scan-and-Lock mechanism, a continuous transmission with channel hopping mechanism proposed in OF∂COIN [7] and eOF∂COIN [9], maintains usable links under interference. By using Force-Initiated mechanism, not only the host but also the synchronization agents are able to initiate the network, which is quite different from the mechanisms in most current CT-based protocols. It was applied in eOF∂COIN [9] to decentralize the network, thereby improving reliability. We name the CT-based protocol with the Scan-and-Lock mechanism and the Force-Initiated mechanism as DeCoT [8].

Each event in these scenarios of previous competitions can be described with ONE bit. That is to say, the payload is so tiny that we can repeat the payload continuously to guarantee a high reliability. Obviously, as we have done in [9], putting all the events from different sources into one packet does not drastically lengthen the payload. However, the scenario of this year is more challenging. An event could be several bytes rather than one bit. That means simple repetitions of an event in the network is not feasible and energy-efficient since each event can not be represented as ONE bit any more. The traffic also would be more dynamic, i.e., the period between two events would be either 1 s or 30 s. To this end, we propose DeCoT+, which combines DeCoT with a **Con**sistency Strategy and a **Ne**twork **C**oding (ConNeC).

2 DeCoT+

DeCoT is based on CT and supports many-to-all communications. It exploits Scan-and-Lock mechanism and Force-Initiated mechanism. On the fundamental of DeCoT, DeCoT+ combines the consistency strategy with the network coding. In this section, we briefly present DeCoT+.

2.1 Consistency Strategy

Considering such a scenario with eight sources, each source has 4-byte packets to transmit. That is to say, a direct concatenation of these packets requires at least a payload of 32 bytes, if there is no data compression used. Even worse, some source nodes probably have 64-byte packets to transmit at the same time. It is impossible to put all the packets into one payload due to the limitation of the maximum length of the payload in IEEE 802.15.4 standard. Therefore, we need

International Conference on Embedded Wireless Systems and Networks (EWSN) 2019
25–27 February, Beijing, China

ISBN: 978-0-9949886-3-8

a consistency strategy that all nodes in the network agree in advance and abide by. The goal of the consistency strategy is to let the information, which is unknown to the sink, to be flooded to the sink as soon as possible. For example, in a CT period, both node A and node B have packets to send to the sink at the same moment. According to the consistency strategy, packets from node A always have a higher priority. Therefore, the payload would be filled with the packet from node A. Eventually, in this period the packet from node A is forwarded by relays and received by the sink. The packet from node B would be scheduled to be forwarded in the following period. However, the specific consistency strategy can be optimized according to a concrete application scenario and benchmarks of the protocol.

2.2 Network Coding

Assuming that we put a 64-byte payload in one packet of IEEE 802.15.4, i.e., to send a long packet directly rather than to split it into multiple small packets, all the nodes need to forward this long packet in one single period. That means, the period would have to be long. The sink needs to wait for a relative longer period of time, e.g., another period, if the long payload is not received successfully in the current period. Then, the latency would increase in this case. Consequently, we decide to divide a long packet into several small blocks to deliver.

Some approaches are based on a handshaking mechanism, e.g., Crystal [3, 4], work well when the handshaking packet can be received, such as an acknowledgement (ACK) packet. However, this mechanism is not dependable enough under harsh interference. Therefore, relying on an ACK might not be reliable under intensive interference. Compared to the handshaking mechanism, the intra-session network coding is more reliable, because no handshaking packet is required at all.

In summary, we divide a long packet into several small blocks to deliver. Then we apply an intra-session network coding, e.g., LT Codes [6], to those blocks. The sink can recover the long packet after a certain amount of coded blocks have been received.

2.3 Many-to-all Communication

Data collection is a many-to-one communication scenario. This does not mean that the source in the network does not need to communicate with other sources. On the contrary, one source is required to give away the opportunities to others if it has nothing to send. One source can repeat a message for a number of times to guarantee the reliability when others have nothing new to send. Thus, in this competition scenario (a many-to-one scenario), we can not avoid many-to-all and many-to-many communications. And we believe that our protocol would benefit a lot from them. As mentioned above, DeCoT+ does not rely on ACK to ensure the high reliability. However, the ACK from the sink to the others helps to optimize the allocation of the network resources. That is to say, to make the allocation reasonably, DeCoT+ disseminates the ACK from the sink representing from which source the message has been received.

2.4 Node Failure

A dependable network should be able to recover from any failure states. If a network is partitioned unexpectedly by interference, the traditional centralized CT protocols such as Glossy [2], LWB [1], Crystal [3, 4] and Chaos [5] can not even complete the initialization phase [8]. Generally, the host in these protocols is the sink in the scenario of data collection. Packets from the sink in these protocols can not reach all the nodes at all. That means these nodes consume energy without any contribution until they are initialized, i.e., synchronized with the host.

Relay nodes, in the assumed scenario, may suffer a power failure at any time and reboot after a random period of time. To let the rebooted nodes be initialized as soon as possible, the Force-Initiated mechanism is used.

3 Preliminary Result

We conducted extensive experiments in the first topology (Layout 1). In all the scenarios – even when the interference level is the most intensive – we can achieve a reliability of more than 95%, with the payload of 64 bytes and the message generation period of five seconds. A main lesson was learned in the preparation phase. A high reliability can be achieved if dividing a long packet into several short blocks in the harsh interference (Level 3). However, the latency increases especially when the number of source nodes increases. Therefore, the reliability and the latency needs to be balanced when the inter-network coding is applied in our protocol.

4 References

[1] F. Ferrari, M. Zimmerling, L. Mottola, and L. Thiele. Low-power wireless bus. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems (SenSys)*, pages 1–14, New York, NY, USA, 2012. ACM.

[2] F. Ferrari, M. Zimmerling, L. Thiele, and O. Saukh. Efficient network flooding and time synchronization with Glossy. In *Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 73–84, April 2011.

[3] T. Istomin, A. L. Murphy, G. P. Picco, and U. Raza. Data prediction + synchronous transmissions = ultra-low power wireless sensor networks. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems (SenSys)*, pages 83–95. ACM, 2016.

[4] T. Istomin, M. Trobinger, A. L. Murphy, and G. P. Picco. Interference-resilient ultra-low power aperiodic data collection. In *Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 84–95. IEEE Press, 2018.

[5] O. Landsiedel, F. Ferrari, and M. Zimmerling. Chaos: Versatile and efficient all-to-all data sharing and in-network processing at scale. In *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, pages 1:1–1:14, New York, NY, USA, 2013. ACM.

[6] M. Luby. LT codes. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 271–280, Nov 2002.

[7] X. Ma, W. Tang, W. He, F. Zhang, and J. Wei. Using OF∂COIN under interference. In *Proceedings of the International Conference on Embedded Wireless Systems and Networks (EWSN), Dependability Competition*, 2017.

[8] X. Ma, P. Zhang, X. Li, W. Tang, J. Wei, and O. Theel. DeCoT: A dependable concurrent transmission-based protocol for wireless sensor networks. *IEEE Access*, 6:73130–73146, 2018.

[9] X. Ma, P. Zhang, W. Tang, X. Li, W. He, F. Zhang, J. Wei, and O. Theel. Using enhanced OF∂COIN to monitor multiple concurrent events under adverse conditions. In *Proceedings of the International Conference on Embedded Wireless Systems and Networks (EWSN), Dependability Competition*, Feb 2018.