FALCON: An Accurate Real-time Monitor for Client-based Mobile Network Data Analytics

Robert Falkenberg and Christian Wietfeld
Communication Networks Institute, TU Dortmund University, 44227 Dortmund, Germany
Email: {Robert.Falkenberg, Christian.Wietfeld}@tu-dortmund.de

***Abstract*—Network data analysis is the fundamental basis for the development of methods to increase service quality in mobile networks. This requires accurate data of the current load in the network. The control channel analysis is a way to monitor the resource allocations and the throughput of all active subscribers in a public mobile radio cell. Previous open-source approaches require either ideal radio conditions or long-term observations in order to obtain reliable data. Otherwise, the revealed information is polluted by spurious assignments with random content. In this paper, we present a new open-source instrument for Fast Analysis of LTE Control channels (FALCON), which combines a novel shortcut-decoding approach with the most reliable techniques known to us to reduce the aforementioned requirements significantly. Long-term field measurements reveal that FALCON reduces errors in average by three orders of magnitude compared to currently the best approach. FALCON allows observations at locations with interference and enables mobile applications with single short-term tracking of the local load situation. It is compatible with numerous software defined radios and can be used on standard computers for a reliable real-time analysis.**

I. Introduction and Related Work

Data analytics, in conjunction with machine learning, is envisioned to empower future mobile networks to predict and avoid congestions through pro-active traffic steering and load balancing. At the same time, the concept of the network slicing in the fifth generation (5G) mobile communication system enables vertical industries to provide tailored services which span over multiple, partially virtualized network components on a shared infrastructure. With the presence of large sets of heterogeneous service quality requirements in a dynamically changing network, data analytics play a major role not only for network maintenance, but also for avoiding Service Level Agreement (SLA) violations with far-reaching consequences. For this purpose, the 3rd Generation Partnership Project (3GPP) has recently begun to standardize interfaces for a Network Data Analytics Function (NWDAF) [1], which allows network components, e.g. the Policy Control Function (PCF), to subscribe notifications for events like slice congestions.

In order to not limit the development of these functions to simulated scenarios, researchers also need access to detailed load information of current live networks. From this information can be derived realistic load profiles, models for user behavior and the evaluation of prediction methods in the field. A recent study required knowledge of the cell load for an in-depth analysis of bottlenecks in public Long Term Evolution (LTE) networks [2]. Traces of the cell load were used to evaluate the performance of Carrier Aggregation (CA) in LTE-Advanced (LTE-A) [3] or to measure the spectral efficiency in the field [4]. Artificial neural networks were used in [5] to implement a client-based data rate prediction depending on the current network load. This information can further improve the efficiency of context-predictive vehicle-to-cloud communication [6] and avoid transmissions in congested cells.

In order to obtain the necessary information about the cell load, the Physical Downlink Control Channel (PDCCH) of an LTE cell can be analyzed. The channel signalizes the resource allocation and the Modulation and Coding Scheme (MCS) with a resolution of 1 ms to individual participants. Although these messages are not encrypted, only the addressed User Equipment (UE) can verify the integrity of the decoded message because the Cyclic Redundancy Check (CRC) sequence is scrambled with the Radio Network Temporary Identifier (RNTI) of the UE. The main difficulty of the control channel analysis is thus the reconstruction of the set of active RNTIs.

Besides expensive commercial tools with specialized hardware [7] and proprietary software solutions [8], there are also some open-source attempts based on Software-Defined Radios (SDRs). These are LTEye [9], Online Watcher for LTE (OWL) [10], and our previous work for Client-based Control Channel Analysis for Connectivity Estimation (C^{3}ACE) [11], which are all described in more detail in the following section. Fig. 1 provides an overview of the key properties of these approaches with regard to operating conditions (signal quality and monitoring time) and lists use cases which require a cell-load monitoring.

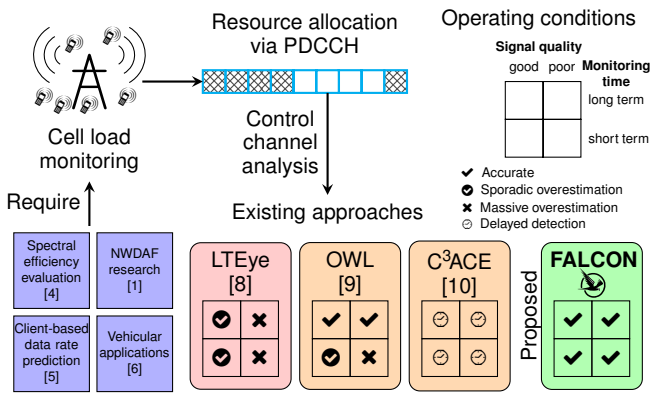

Fig. 1. Overview of existing approaches for monitoring the cell load and their suitability for different operating conditions. The proposed method FALCON enables accurate short-term monitoring even in non-ideal radio conditions.

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

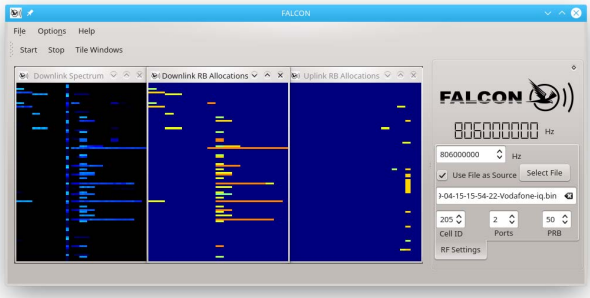

Fig. 2. Screenshot of FALCON's live resource allocation viewer in action. Three waterfall plots show the current signal magnitude of the cell signal (left) and the decoded resource block allocations for the downlink (center) and the uplink (right) at subframe level. Individual users are colored differently. The downlink allocations perfectly match the actual spectral occupation.

To the best of our knowledge, OWL is currently the most reliable open-source instrument for continuous long-term monitoring, as it tracks the initial RNTI assignments of new UE that enter the cell. To discover RNTIs from passed assignments, it falls back to LTEye's re-encoding technique, which is explained in Sec. II-C. However, re-encoding is very sensitive to interference and noise so that OWL and LTEye both require almost perfect radio conditions to produce a reliable output in short term observations. C^{3}ACE, on the other hand, tracks the activity of supposed RNTIs with a histogram and only accepts those RNTIs that exceed a predefined occurrence threshold in the histogram. While this approach is robust against spurious detections, the time required to exceed the threshold leads to a delayed detection of new UE and UE with low activity may stick below the threshold.

In this paper, we present FALCON[1]: Fast Analysis of LTE Control channels, an improved, further developed combination of the existing methods, which is suitable for both, long-term and short-term monitoring of LTE resource allocations in non-ideal radio conditions. FALCON is completely open-source and it is released under Affero General Public License v3.

The rest of the paper consists of an introduction in control channel analysis and the involved challenges (Sec. II), an overview of the FALCON suite with the involved Downlink Control Information (DCI) validation methods (Sec. II-C), and a comparative evaluation of FALCON against OWL (Sec. IV). Finally, a conclusion is drawn in Sec. V.

II. Control Channel Analysis

In this section, we give a brief introduction into resource assignment functions in LTE/LTE-A networks to provide an understanding of the challenges in monitor cell load through observations. We present the key methods used by existing approaches and discuss the applicability in 5G.

[1]The code is available at https://github.com/falkenber9/falcon

A. Resource Assignments

In LTE/LTE-A networks, the evolved NodeB (eNodeB) centrally governs radio resources in terms of Resource Blocks (RBs) which are dispensed to the attached UEs. Except for the initial network access, namely Random Access (RA), the entire communication happens according to explicit resource assignments by the eNodeB. These assignments, namely DCI, are signaled via PDCCH in the first symbols of each subframe once in 1 ms. DCI from PDCCH in subframe n addresses the current subframe n for the downlink and subframe $n+4$ in uplink direction. LTE-A extends this signaling by an optional Enhanced PDCCH (EPDCCH), which can be located in sets of RBs distributed along the entire resource grid in order to reduce interference and congestion of the PDCCH control region in very dense environments or heterogeneous networks.

As shown in Fig. 3, the PDCCH region consists of several Control Channel Elements (CCEs), which are occupied by the encoded DCI for distinct UEs. Depending on radio conditions of particular UE, the eNodeB selects a suitable aggregation level $L \in \{1, 2, 4, 8\}$ and fills the encoded DCI into L consecutive CCEs. Each DCI is appended by a 16-bit CRC checksum, which is additionally scrambled (via bitwise XOR) by the particular UE identity, i.e. the RNTI, of the same length. The assignment of RNTI is performed during the RA procedure in a not encrypted Random Access Response (RAR) message. Further sets of RNTIs are defined to serve specific purposes, e.g. for system information (SI-RNTI = `0xFFFF`) or paging (P-RNTI = `0xFFFE`).

Lastly, the standard defines various DCI formats [12] for allocations in different transmission modes and which differ in their payload size. The eNodeB applies channel coding and rate matching to fit the encoded DCI exactly into the selected number of CCEs.

B. Blind Decoding and Search Space

The PDCCH has no table of contents and neither DCI format nor aggregation level L is signaled explicitly. Therefore, the UE has to repeatedly perform a blind decoding of the PDCCH contents under the assumption of a certain DCI format and L. Only after a candidate has been decoded, the CRC reveals a hit if the RNTI equals to the CRC value.

In order to limit the number of decoding attempts, the standard defines two search spaces, which comprise two subsets of all possible locations and associated aggregation levels. The first search space is UE-specific and comprises 16 locations which are scattered along the PDCCH. These depend on the RNTI and the current subframe number $0 \ldots 9$ according to the search space function [13]. The second search space is common for all RNTI and comprises 6 locations in the first CCEs of a PDCCH. Besides UE-specific data, this search space also carries DCI for paging, system information and random access. Ultimately, the UE only monitors DCI formats for its current transmission mode. Carrier Aggregation in LTE-A may lead to additional UE-specific search spaces for each component carrier in case of cross-carrier scheduling.

TABLE I
OVERVIEW OF DCI VALIDATION TECHNIQUES USED BY NON-COMMERCIAL PDCCH DECODERS

	Decoder			
Technique	**LTEye** [9]	**OWL** [10]	**C³ACE** [11]	**FALCON**
Signal power	X	X	–	X
Re-encoding	X	X	–	–
RAR tracking	–	X	–	X
RNTI histograms	–	–	X	X
Search space coherence	–	X*	X	X
Short-cut (**new**)	–	–	–	X

*Added in a later release

C. Approaches and Challenges in DCI Validation

The major challenge of decoding the global set of DCI in a monitored cell is related to the concept of blind-decoding. In contrast to a regular UE, an external observer has no knowledge about currently assigned RNTIs, individual transmission modes and the associated subset of DCI formats. Therefore, rules for search space reduction are not applicable here. Instead, any possible location needs to be decoded with respect to any potential DCI format and aggregation level. This results in a large set of mostly false candidates for the same sequence of CCEs. However, since the CRC is scrambled with the RNTI of the addressee, a CRC validation presupposes knowledge of valid RNTIs. To overcome these limitations, researchers have proposed different approaches to validate DCI candidates and reconstruct the set of active RNTIs:

Signal power detection greatly reduces the number of blind decoding attempts by disqualifying any CCEs which undershoot a predefined average signal level. However, Inter Cell Interference (ICI) may lead to a number of false-positive classifications especially if the signal is received at the edge between two sectors.

Re-encoding the decoded DCI and comparing the output with the initial bit sequence was proposed with LTEye [9] and is also included as a fall-back in OWL [10]. Candidates are regarded as valid if the encoded sequences match in orders of at least 97 %. However, our measurements show that this approach is error-prone in the presence of interference, noise or in case of imperfect synchronization which all lead to massive false detections. Therefore, this approach is not included in FALCON.

RAR tracking was introduced with OWL [10] as a reliable method for long-term observations which captures initial RNTI assignment messages. However, short-term observations lack unseen assignments in the past, since this method discovers only those RNTIs which have been assigned during the observation period.

RNTI histograms have been presented with C³ACE [11] as a method for DCI validation in short-term observations, which is less sensitive to the radio conditions. Given a short time window T, valid RNTI appear more frequently in that interval while RNTI from false candidates are evenly distributed along the 16-bit value range. If an RNTI exceeds a certain threshold k, the corresponding DCI is assumed as valid. The values T and k are a trade-off between the false-positive probability and the required minimum UE activity to be detected. A threshold value that is set too high filters out subscribers who are very rarely scheduled.

Search space coherence can be validated by reverse application of the search space function (cf. Sec. II-B) after decoding. Since the eNodeB never places DCI outside the associated search space, outlying candidates can be safely discarded. This method was introduced with C³ACE and was added to OWL afterward. With a search space of 22 candidates for a regular UE (i.e. 6 common + 16 UE-specific) and the maximum number of 88 CCEs in a 20 MHz cell with one or two antenna ports, this approach filters in average ∼87 % of all false candidates. However, the efficiency of this filter shrinks with the number of CCEs, e.g. down to ∼73 % for 10 MHz with 44 CCEs.

Shortcut decoding is a novel method of the FALCON decoder presented in this paper for the rapid validation of DCI in short-term observations. Uncertain DCI candidates are decoded once more by using only the first half of their occupied CCEs. If this results in the same checksum, the DCI is accepted. The procedure is part of a recursive DCI search, which is explained in more detail in the next section.

Tab. I provides a comparison of FALCON and previous non-commercial decoders with regard to the DCI validation techniques they contain.

D. Applicability in 5G

5G also uses control channels for resource allocation, but DCI is encoded with polar codes with higher spectral efficiency and lower decoding complexity [14]. However, a larger search space increases the number of decoding attempts. The RNTI still comprises 16 bits, but the checksum of the DCI has been increased to 24 bits. After subtracting 3 bits for list decoding of the polar codes, at least 5 bits are not scrambled and can be used for a vague validation without RNTI knowledge [15]. It can be supported by an RNTI histogram to discover the active set. However, an additional requirement is the localization of the Control Resource Sets (CORESETs), which can be located anywhere in the resource grid, analogous to the EPDCCH. If the CORESET makes use of beamforming, a higher receive signal strength may be required to decode the contents correctly.

III. STRUCTURE OF FALCON

In this section, we introduce FALCON: Fast Analysis of LTE Control channels. FALCON comprises an open source software suite for real-time monitoring of LTE resource allocations based on PDCCH decoding over the air interface. Besides the decoder and a visualization tool, the software includes a signal recorder with integrated network probing and a remote controller for synchronized capturing of multiple

cells or Mobile Network Operators (MNOs). Additionally, FALCON includes a port of OWL's recorder and decoder, the latter of which can also be run in LTEye mode.

The software is based on the SRSLTE library [16] v18.12 and is kept separated from the underlying library in order to benefit from future updates without a tedious merge and prepares the integration of a 5G library.

FALCON can be executed on an x86-based general purpose computer running a generic Linux kernel. Any software defined radio supported by SRSLTE can be used to perform over-the-air measurements. The software is tested with the USRP B210 by Ettus Research. Without any radio, the software decoders are also capable to process and visualize recorded signals from a file.

A. Signal Recorder with Network Probing

The signal recorder is an extended version of OWL's recorder and capable of synchronizing to a particular LTE cell and capturing the raw I/Q samples for a predefined time interval. Data is either written directly to a hard disk or buffered into Random Access Memory (RAM) and written to a hard disk when finished. Buffering greatly reduces the IO-load on the system and avoids the loss samples from the radio transceiver that would otherwise lead to a loss of cell synchronization. As buffering consumes 88 MB of RAM per second for a 10 MHz cell, it is applicable for short-term recordings below one or two minutes.

The monitored cell is selected automatically, manually or corresponding to the serving cell of an external modem. That external modem is also used to produce cell traffic for measurements of the achievable throughput and the involved transmission power. These results are stored together with cell information and quality indicators such as Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ). Simultaneous capturing with multiple recorders can be synchronized via Ethernet by an additional remote controller process.

B. Real-Time Decoder

FALCON's core component is the PDCCH decoder, which is capable of tracking either an online LTE signal or an offline recording and reliably decodes any resource assignments from the cell's PDCCH in real time. Like a regular UE, it synchronizes to a cell and configures the receiver according to the cell configuration. Instead of performing an attach, the decoder remains passive and goes ahead with PDCCH analysis. This includes a systematic decoding of any possible location among the CCEs (including every aggregation level) with all potential DCI formats. As stated in Sec. II-C, the major challenge is the efficient reconstruction of the valid RNTI set for a reliable validation of the decoded DCI candidates. Similar to OWL, FALCON decodes only locations with a sufficient signal power in all covered CCEs and checks the coherence between the candidate's RNTI and the corresponding search space. It also keeps track of any RAR messages that contain RNTI assignments for newly joined UEs which are immediately added to the active set [10]. However, to quickly bootstrap the list of already active RNTI, FALCON does not rely on LTEye's and OWL's re-encoding technique, that is sensitive to the channel conditions. Rather, FALCON combines RNTI histograms from C^{3}ACE with the new recursive shortcut validation technique:

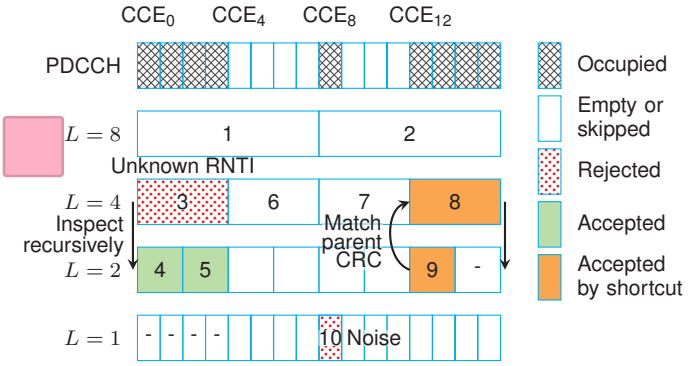

Fig. 3. Illustration of FALCON's new recursive PDCCH decoding procedure. Possible DCI locations are inspected sequentially starting with the largest aggregation level L=8. Locations containing empty CCEs are skipped (1, 2). Checked locations without any known RNTI (3) are split into two halves and are examined recursively with $L/2$ (4, 5). Locations that overlap any match are also skipped (-). If a shortened location (9) decodes the same uncertain RNTI as the parent (8), the candidate is accepted immediately.

Instead of processing all possible locations as breadth-first search with descending aggregation levels like OWL, FALCON performs a depth-first search as illustrated in Fig. 3. If a decoded location with aggregation level L does not contain any candidate from the active set (cf. 3), the location is split and inspected recursively using $L/2$ (cf. 4 and 5) until valid candidates are found or $L = 1$ is reached. When the recursion does not detect any valid DCI, all coherent but rejected RNTIs along the recursion path are added to a histogram of uncertain RNTIs. If an RNTI appears at least five times within a sliding window of 200 ms, it is added to the active set [11]. A shortcut is taken, if decoding a shortened location (cf. 9) results in the same RNTI as the parent (previously rejected) candidate. In this case, the DCI is accepted and the RNTI is immediately added to the active set. With this method, the majority of RNTIs is detected at first occurrence. This shortcut works because the eNodeB implements rate matching of encoded DCI by circularly writing the encoded sequence into L consecutive CCEs [12].

Finally, the decoder writes the content of validated DCI into a file or visualizes the resource assignments in the subsequent viewer.

C. Real-Time Resource Allocation Viewer

For a live visualization of the cell activity or for a playback of a previous recording, the PDCCH decoder is also embedded into an OpenGL-accelerated Graphical User Interface (GUI) as shown in Fig. 2. Resource allocations for uplink and downlink are displayed at subframe level and can be compared with the allocation in the spectrum. Additional metrics, such as average throughput or activity of individual users, can also be displayed.

D. Comparative Software and Fairness

In order to allow a fair comparison between FALCON, OWL and LTEye[2], OWL was separated from the outdated library and adapted to the current version of SRSLTE. To ensure that the port does not break the original functionality, numerous records were analyzed by both the original and ported version. Both versions lead to an identical classification of all candidates if the resolution of the Viterbi decoder is equalized. Only negligible differences in the content of some decoded DCI were found, which are the result of corrected bugs and which have no influence on the functionality. The computational complexity of OWL and FALCON is almost identical. Both require approx. 2 s to analyze a record of 5 s.

E. Privacy

Although the decoding of DCI gives the impression that sensitive information is being detected, the privacy of cell users is not at risk. RNTIs are volatile identifiers and are released after a few seconds of inactivity. The payload within the allocated resources is encrypted and cannot be decrypted without knowledge of the secret keys.

IV. Evaluation and Results

Validating the correct function of a PDCCH decoder is a major challenge. A comparison between spectral occupancy and decoded resource allocations does not provide a reliable evaluation metric due to activity in neighboring sectors. The same applies to the comparison of occupied and decoded CCEs due to overlapping PDCCHs of the neighbors. In addition, the degree of redundancy of the DCI corresponds to the radio conditions of the addressed subscriber. Therefore, if the monitored signal is weak, losses of some DCI must be expected. However, this should by no means lead to the acceptance of corrupt DCI with random content.

A reliable metric is the occurrence of collisions due to the erroneous multiple allocations of the same RBs within a subframe. Multi User-MIMO (MU-MIMO) assignments must be excluded from this, but we have not found any assignments with the corresponding DCI format 1D anyway.

Furthermore, we found in our experiments that the monitored base stations assign new RNTIs sequentially. As a result, active RNTIs accumulate in a small value range, especially since RNTIs are released after a short period of inactivity. The following describes the setup of a long-time measurement, which is then evaluated against the above criteria.

A. Measurement Setup

For the evaluation of FALCON, we set up a measurement system with three synchronized recorders to monitor three cells from different MNOs simultaneously. Recordings are triggered in intervals of 5 min to capture 5 s from each cell and are directly processed by the decoders FALCON and OWL. We removed recordings that suffered a synchronization loss.

The recorders were placed in an office next to an insulating window in line of sight to a building which is populated by eNodeBs from all three MNOs (cf. Fig. 4). Although the location is identical, the eNodeBs differ in antenna orientation and transmit power. This results in different received signal levels at the measurement point as listed in Tab. II. The line of sight is crossed by a highway which leads to the German city Dortmund and is intensively used by commuters during the rush hours. The measurement covers a period of five days, including a weekend, a public holiday and a working day.

[2]LTEye is mimicked by OWL with disabled RAR tracking (cf. Tab. I)

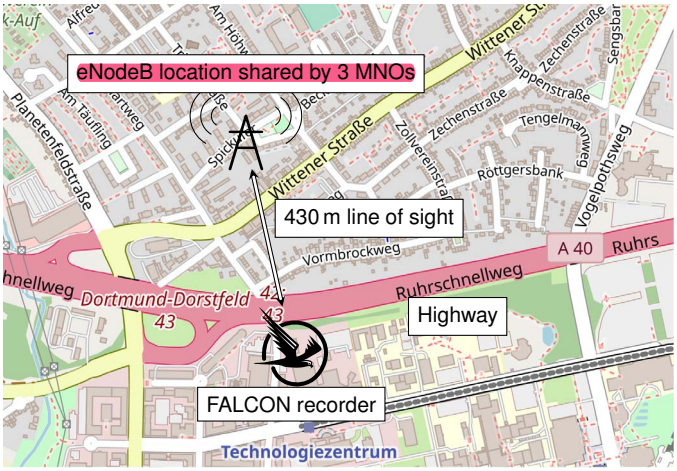

Fig. 4. Map of the measurement setup and the three monitored eNodeBs. Despite the shared location, the eNodeBs differ in transmission power and antenna orientation. The cells cover a highway which is densely populated during the rush hours. (Map: ©OpenStreetMap contributors, CC BY-SA)

TABLE II
Ke[redacted]work parameters of the long-term measurement.

	MNO1	MNO2	MNO3
Signal Quality	Good	Fair	Poor
Frequency	800 MHz	800 MHz	800 MHz
Bandwidth	10 MHz	10 MHz	10 MHz
RSRP (average)	−91.23 dBm	−99.23 dBm	−107.69 dBm
RSRQ (average)	−7.11 dB	−10.05 dB	−14.39 dB
Measurements	1389	1227	1150

TABLE III
Average fraction of subframes with contradictory resource allocation because of false detections. Figures in percent.

	MNO1	MNO2	MNO3
Signal Quality	Good	Fair	Poor
Uplink			
OWL	0.002 %	0.001 %	0.024 %
FALCON	0.000 %	0.000 %	0.001 %
Downlink			
OWL	0.284 %	0.516 %	**2.527 %**
FALCON	0.000 %	0.001 %	**0.005 %**

B. Reliability and False Detections

Our measurements showed that especially poor radio conditions provoke false DCI detections which lead to conflicting allocations of the same resources to multiple RNTIs in the same subframe. Tab. III shows the average fraction of subframes that contained such a collision in uplink and downlink direction. The results show, that in case of poor radio conditions (MNO3) FALCON outperforms OWL in average by three orders of magnitude. Compared to the downlink, the probability of uplink collisions is smaller because uplink allocations are bound to a single DCI format while the remaining DCI formats carry downlink allocations. Since not every spurious DCI causes an actual collision, the collisions only indicate a lower bound for false detections.

Therefore, we inspect the number of occurrences of each RNTI in the decoded time interval in more detail. The underlying assumption is that spurious DCI, which is mistakenly assumed as valid, contains a random payload and a random CRC that is interpreted as RNTI. These spurious RNTIs are scattered uniformly along the entire value range of 2^{16} with a very low frequency, each. The low frequency is a consequence of the small probability hitting the same RNTI multiple times across a number of coin toss experiments [11].

Based on the decoded DCI by both decoders, we computed the set of RNTIs which appeared during a monitored interval of 5 s and counted their occurrences. Fig. 5 shows the frequency and the distribution of discovered RNTIs for three consecutive recordings in the morning rush hour of a working day for the case of poor radio conditions. In particular, the probing modem (cf. Sec. III-A) reported an RSRP of 109 dBm and an RSRQ of −14 dB for this example. We can see in each chart that the most active RNTIs concentrate in a small and dense range of values. In contrast to FALCON, OWL additionally reports a huge set of RNTIs with a very small frequency of mostly less than three occurrences. These are evenly distributed across the full value range and match the previous assumptions of random CRCs. Hence, these RNTIs are likely false detections from the re-encoding approach.

The peak region, however, is not bound to a fixed interval but moves with time in ascending order along the value range. To illustrate the progression, we added help lines to Fig. 5 to highlight the peak regions from recordings in the same cell five and ten minutes earlier. This indicates that the base station incrementally assigns RNTIs to new UE that join the cell via handover or wake up from idle mode. In the given example the RNTI number has advanced by 7552 in 10 minutes which represents a mean RNTI assignment rate of 12.6 RNTIs per second. Furthermore, each assignment involves an RA procedure in one of the serving sectors of the cell. Hence, the RNTI progression rate must correspond to the monitored number of activities by RA-RNTIs. The RA activity in the 10 min interval is in average 2.66 assignments per second. Assuming an equal activity in all six cell sectors (three in band 20 and three in band 7), the extrapolated value of $6 \cdot 2.66 = 15.96$ slightly overshoots the RNTI progression rate.

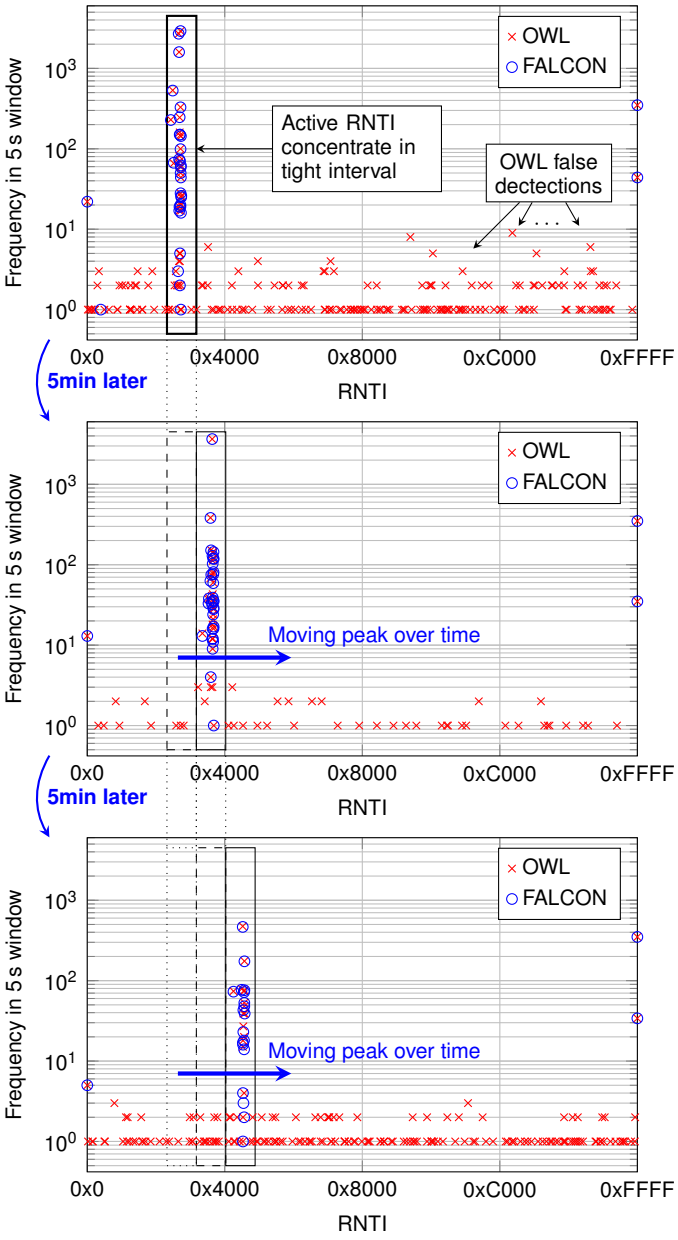

Fig. 5. Distribution and Frequency of RNTIs from detected DCI by OWL and FALCON for three subsequent recordings over 5 s in intervals of 5 min. The recordings were made at poor radio conditions (MNO3, RSRP: 109 dBm, RSRQ: −14 dB) during rush hour. True RNTIs concentrate in a dense peak region that moves rightwards over time. This indicates a sequential RNTI assignment by the eNodeB and a high user fluctuation in the cell. In contrast to FALCON, OWL detects numerous false RNTIs which form an evenly distributed noise floor.

However, only four sectors are directed towards the populated highway, while the remaining sectors cover a residential area. Considering only those four sectors for the extrapolation, we receive a rate of 10.64 assignments per second, which slightly undershoots the progression rate. Consequently, the two estimations tightly enclose the RNTI progression rate and confirm the sequential RNTI assignment by the base station.

Finally, the peak region of active RNTIs sharply dies away towards smaller (and older) values for both decoders. This indicates a very short activity time of the UEs for the purpose

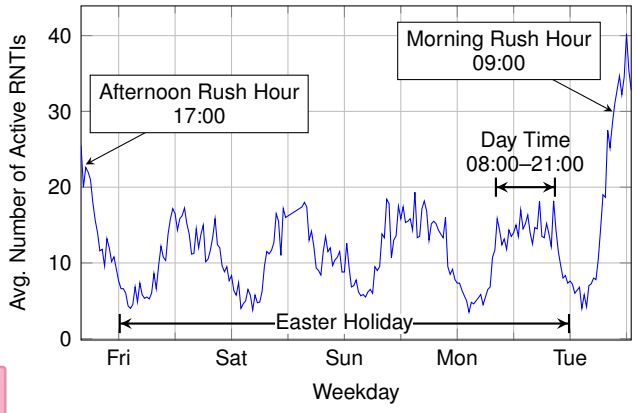

Fig. 6. Application example of FALCON showing the average number of concurrently active subscribers in a cell of MNO2 during the Easter Weekend. The graph shows a typical slope of ∼15 concurrent UEs during day time on a holiday and more than 30 UEs during rush hours on a business day.

of a data exchange followed by a handover into the next cell along the highway or releasing the RNTI due to inactivity. Furthermore, the distribution and frequency of the RNTI noise using OWL have an equal shape on both sides of the peak region with no significant cumulation on the left side. This indicates, that FALCON does not filter out any meaningful DCI for RNTI in the value range beyond the peak region.

C. Application Example

An application example of FALCON is given in Fig. 6 which shows the average number of simultaneously active UEs in a cell of MNO2 during our campaign. We define the number of active UEs as the cardinality of the set of RNTIs which are scheduled at least once in the monitoring interval of 5 s. Due to a large number of samples, we averaged the results in bins of 30 min. The chart shows approx. 15 concurrent UEs during day time on a holiday and approx. 5 UEs during night. Business days, especially during rush hours, are characterized by a significantly higher number of concurrent UEs.

V. Conclusion

In this work, we presented FALCON, an open-source instrument for Fast Analysis of LTE Control channels in public LTE networks. FALCON reliably obtains the entire resource allocations of a monitored cell in real-time. The novel approach of shortcut-decoding provides a fast integrity check of DCI addressing previously unseen RNTIs which almost instantly reconstructs the list of currently active RNTIs in the cell. This method fully replaces the re-encoding validation technique used by LTEye [9] and OWL [10], that is responsible for numerous false detections under less than ideal radio conditions. With the support of the histogram-based validation of uncertain DCI candidates, FALCON maintains its accuracy even in case of a weak signal. According to our measurements, FALCON reduces the probability of downlink RB collisions by three orders of magnitude in case of a poor signal. Therefore, FALCON paves the way for reliable short-term monitoring, e.g. to supply mobile vehicles with information about cell congestions and increase the prediction accuracy for opportunistic vehicle-to-cloud transmissions. It is a powerful solution for the analysis of network congestions and a key enabler for the development of NWDAF. It allows other researchers to derive realistic traffic models from public networks, independent from the network operators, and without the requirement of expensive hard- and software.

Acknowledgment

Part of the work on this paper has been supported by Deutsche Forschungsgemeinschaft (DFG) within the Collaborative Research Center SFB 876 “Providing Information by Resource-Constrained Analysis”, project A4.

References

[1] *3GPP TS 29.520 - Network Data Analytics Services (Release 15)*, 3rd Generation Partnership Project Technical Specification, Rev. V15.2.0, Dec. 2018. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/29_series/29.520/

[2] A. Balasingam, M. Bansal, R. Misra, K. Nagaraj, R. Tandra, S. Katti, and A. Schulman, “Detecting if LTE is the bottleneck with BurstTracker,” in *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom ’19)*. Los Cabos, Mexico: ACM, Oct. 2019.

[3] N. Ludant, N. Bui, A. G. Armada, and J. Widmer, “Data-driven performance evaluation of carrier aggregation in LTE-Advanced,” in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct. 2017.

[4] J. Um, I. Kim, and S. Park, “A method for analyzing spectral efficiency using real-field measurement data,” in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2018.

[5] R. Falkenberg, K. Heimann, and C. Wietfeld, “Discover your competition in LTE: Client-based passive data rate prediction by machine learning,” in *IEEE Globecom*, Singapore, Dec. 2017.

[6] B. Sliwa, R. Falkenberg, T. Liebig, N. Piatkowski, and C. Wietfeld, “Boosting vehicle-to-cloud communication by machine learning-enabled context prediction,” *IEEE Transactions on Intelligent Transportation Systems*, Jul 2019.

[7] J. Um, I. Kim, and S. Park, “Implementation of platform for measurement and analysis on LTE traffic and radio resource utilization,” in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Jan. 2019.

[8] Software Radio Systems, “AirScope — SRS,” May 2019. [Online]. Available: https://www.softwareradiosystems.com/tag/airscope/

[9] S. Kumar, E. Hamed, D. Katabi, and L. Erran Li, “LTE radio analytics made easy and accessible,” in *Proceedings of the 2014 ACM Conference on SIGCOMM*. New York, NY, USA: ACM, Aug. 2014.

[10] N. Bui and J. Widmer, “OWL: A reliable online watcher for LTE control channel measurements,” in *Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges*, ser. ATC ’16. New York, NY, USA: ACM, Oct. 2016.

[11] R. Falkenberg, C. Ide, and C. Wietfeld, “Client-based control channel analysis for connectivity estimation in LTE networks,” in *IEEE Vehicular Technology Conference (VTC-Fall)*, Montréal, Canada, Sep. 2016.

[12] *3GPP TS 36.212 - Multiplexing and channel coding (Release 15)*, 3rd Generation Partnership Project Technical Specification, Rev. V15.4.0, Dec. 2018. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/36_series/36.212/

[13] *3GPP TS 36.213 - Physical layer procedures (Release 15)*, 3rd Generation Partnership Project Technical Specification, Rev. V15.4.0, Dec. 2018. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/36_series/36.213/

[14] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Transactions on Information Theory*, vol. 55, no. 7, Jul. 2009.

[15] D. Hui, S. Sandberg, Y. Blankenship, M. Andersson, and L. Grosjean, “Channel coding in 5G new radio: A tutorial overview and performance comparison with 4G LTE,” *IEEE Vehicular Technology Magazine*, vol. 13, no. 4, Dec 2018.

[16] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, “srsLTE: An open-source platform for LTE evolution and experimentation,” in *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*, ser. WiNTECH ’16. New York, NY, USA: ACM, Oct. 2016.