PAYMENTS CANADA

IS THERE ANYBODY OUT THERE? DETECTING OPERATIONAL OUTAGES FROM LVTS TRANSACTION DATA

2020-02-25

payments.ca

Is there anybody out there? Detecting operational outages from LVTS transaction data *

Neville Arjani[a] and Ronald Heijmans[b,c]

[a] *Canada Deposit Insurance Corporation*
[b] *De Nederlandsche Bank*
[c] *Payments Canada*

February 25, 2020

Abstract

This paper develops a method to identify operational outages of participants in the Canadian Large Value Transfer System. We define an operational outage as either no or unusual low activity. We test our algorithm against a database of by participants reported outages in order to reduce false negatives. The false positives can be reduced by excluding "outages found" by the algorithm if a participant historically has no payment in a given five minute time interval. Additionally, we can test whether participants do indeed report all their operational outages. The results show that our algorithm works best for the largest participants as they continuously send in payments. Our method can be used by LVTS system operators and overseers to identify sources of operational risks.

Keywords: operational risk, LVTS, financial market infrastructures.
JEL classifications: E42, E58, G21.

*Arjani worked as research director at Payments Canada at the time this research project was carried out. Heijmans is the corresponding author and can be reached at ronald.heijmans@dnb.nl. The authors would like to thank Jan Paulick and Marc Glowka for providing useful comments.

1 Introduction

Financial market infrastructures (FMIs) play a crucial role in the economy. FMIs represent vast financial networks that connect financial intermediaries (and their clients) by means of technology, rules, standards and procedures to facilitate the transfer of value between agents in an economy. Large value payment systems (LVPSs), including real-time gross settlement (RTGS) systems, are a type of FMI that facilitate the exchange, clearing and final settlement of typically large-value and time-sensitive monetary transfers between participating financial intermediaries on their own behalf and that of their clients.[1] They are a critical component of a country's financial system and economy, as they serve as the platform for the implementation of monetary policy, as well as support hundreds of billions of dollars in real and financial transaction activity each day. Needless to say, if these systems do not function properly, they can seriously hinder economic activity. Therefore, FMIs have to live up to high international standards and are generally subject to a strong degree of regulatory and operational oversight, see CPSS (2012).

As LVPSs connect financial intermediaries, interdependencies exist where the actions of one participant in the network will have an impact on the others. For instance, if one participant in the network suffers a technical outage that prevents it from sending payment instructions to other participants in the network as planned, this could result in other participants only being able to fulfill their payment obligations at a higher cost as they must seek intraday funding somewhere else to meet these obligations, e.g., through a central bank intraday credit facility.[2] During the technical outage, the stricken bank serves as a liquidity sink in which incoming liquidity stays trapped on its account and cannot be recycled to the rest of the system. This problem is exacerbated when other participants, either unaware or dismissive of the fact that the stricken bank is unable to send payments,

[1] LVPSs around the world include the US Fedwire and US CHIPS systems, BOJ-NET in Japan, the TARGET2 system in the Euro Area, UK CHAPS, and the Canadian LVTS. Virtually all major economies around the world have adopted a Real-Time Gross Settlement (RTGS) model for their LVPS implementation (Bech and Hobijn (2007).

[2] Incoming payments represent the cheapest source of intraday liquidity for participants in these systems.

continue to funnel transfers to the stricken bank through the network.[3] In the worst case scenario, a technical outage at a participant could result in a gridlock in which no participant is willing or able to make any more payments and waits for others to make the first payment.[4] To mitigate this possibility, timely indication of participant technical outages is key. Therefore, operators of an FMI diligently monitor the activity of their system's participants.[5]

The question we address in this paper is how can operational outages of individual participants in the Canadian Large Value Transfer System (LVTS) be detected in a more timely manner. Even though LVTS participants are required by the LVTS Rules to inform the system operator within 15 minutes of detecting a technical disruption in their ability to send and/or receive payments, anecdotal evidence suggests that this is often not the case, for a variety of reasons.[6] For instance, a participant that is busy trying to restore connectivity may may miss the 15-minute timeline, or forget to contact Payments Canada altogether. In economics parlance, this generates an externality by increasing the risk of financial loss to the system as a whole through this single outage. In all cases, this increases the risk of financial loss associated with operational outages. Given the strong seasonal patterns observed in the LVTS on an intraday, daily, monthly and even quarterly basis, coupled with the prospective real-time availability of these data to Payments Canada and in the development of machine learning algorithms focused on anomaly detection, it seems that more timely and accurate detection of operational outages in the LVTS is certainly possible. This has the potential to reduce the cost associated with such events, thereby reducing the risk profile of the system as a whole.

[3] This could be due to a healthy participant thinking that the stricken bank will recover quickly.

[4] Liquidity injections are still possible of course (e.g., central bank lending facility) in this scenario, but they too carry a financial cost.

[5] Moreover, some system operators may choose to impose strict operational availability requirements on participants in the network (as is the case in Canada), which are subject to compliance protocols if not adhered to. As well, given the importance of these systems, there are often manual or other special back-up facilities that might be available for an affected participant to continue to send value over the network, usually to facilitate any time-sensitive transfers. While these back-up facilities are typically not designed to handle the regular daily flow of participants, they can at least be used to help circulate some liquidity from the affected participant back to the network to help avoid a gridlock scenario. Before backup facilities can be started it has to be known that there is an (operational) problem with a participant.

[6] Non-compliance with this rule garners further follow-up and potential penalty.

To detect operational outages we build on the approach by Glowka et al. (2018) and Klee (2010), who have developed an algorithm for the European RTGS, TARGET2, and the American RTGS, Fedwire, respectively. Glowka et al. (2018) looks in contrast to Klee (2010) at periods of unusual low activity. They argue that in case a participant is not able to send in payment instructions via the standard channels, there may be back up functionalities that allow for making at least a few (very urgent) payments. We modify their approach to make it suitable for the Canadian LVTS. This type of algorithms inevitably leads to potential Type I and Type II errors. A Type I error would be identifying an outage which is not, because the direct clearing member had no (or little) payments to send in. A Type II error would be not identifying an operational outage while in fact there was one. This could be in case the activity of the outage period would be larger than the 1 percentile used. In contrast to Glowka et al. (2018), we have a data base containing the participants' reported outages for two years, which we used to test our algorithm.

Our paper adds to the growing literature for identifying risks for FMIs. Benos and Zimmerman (2012) develop risk indicators measuring the impact of liquidity risk due to operational outages. Their findings indicate that the impact of operational outages on system liquidity has increased since the collapse of Lehman Brothers compared with the observation period before. Berndsen and Heijmans (2020) develop risk indicators based on TARGET2 transaction data that are linked to the principles of financial market infrastructures, that can be used by FMI operators and overseers. Clarke and Hanckock (2013) study how the design of the payment system can impact operational disruptions. Diehl and Müller (2015) study the use of bilateral limits in TARGET2. They find that limits are not actively used and if they are used they are relatively constant over time. Both papers find that liquidity saving mechanisms in a LVPS can reduce the impact of an operational outage. Triepels et al. (2018) implemented a neural network to identify intraday liquidity outliers of an individual bank for TARGET2. Their method can detect starting bank runs from RTGS data. An often investigated aspect of large value payment systems is timing. There may be timing incentives in the payment system, as theoretically described by the game theoreti-

cal model by Bech and Garratt (2003, 2006). Their model has been run in an experimental real life game by Abbink et al. (2017) and Heemeijer and Heijmans (2015). Heijmans and Heuver (2014) study several liquidity aspects that can be derived from RTGS data including payments' timing. The main sources of liquidity they identify from LVPS data are incoming payments, interbank money market loans (which are a special subset of interbank payments), monetary loans (which are transactions with the central bank) and intraday credit (which is backed by collateral), which allows them to make payments event though their account balance is insufficient to make the payment). Kaliontzoglou and Müller (2015) build on their work to derive a payments delay indicator, which can be used for all banks in the Eurosystem. Diehl (2013) explains that free-riding incentives may be behind the timing of payment transactions. Although they find that are no candidates free riding in the German part of TARGET2.

This paper is organized as follows. Section 2 describes the main features of LVTS and the data. Section 3 explains the set of the algorithm to identify the operational outages. Section 4 provides the results of the algotihm and the check with the reported operational outages. Section 5 concludes.

2 Large Value Transfer System

2.1 The system

The Large Value Transfer System (LVTS) is used to facilitate interbank settlement in Canada. Owned and operated by Payments Canada, the LVTS has been in place since 1999 and clears roughly $C200 billion in transaction value each day. This translates to clearing roughly the equivalent of Canadian nominal GDP every nine business days.

The LVTS is best described as a real-time net settlement system. At the heart of the LVTS settlement model stands novation netting, where bilateral settlement obligations stemming from intraday exchange of payment instructions between pairs of participants are immediately extinguished upon LVTS processing and replaced with a multilateral settle-

ment obligation of the sender to the rest of the system. Settlement of multilateral obligations of participants should occur at 18:30 EST on each business day. Settlement takes place in central bank money through daily transfer of value over participants' settlement accounts maintained at the Bank of Canada. Settlement risk stemming from this model is managed via a dual-stream risk model.

The participants can use two different streams in LVTS. It is their choice to which stream they send the payments. The two streams (or Tranches) differ in regard to how settlement risk exposure generated by a participant is controlled. In the first stream, or Tranche 1, any intraday credit exposure posed by a participant to the rest of the system is supported on a dollar-for-dollar basis with financial collateral posted to the central bank by the participant ('defaulter-pays'). In the second stream, intraday credit exposure posed by a participant to the rest of the system is supported by a joint ('survivors-pay') collateral pool and further backed by a central bank commitment. Through a combination of financial collateral, and corresponding bilateral and multilateral net debit limits, the LVTS risk model ensures that, at a minimum, there will always be sufficient collateral value posted to cover the largest possible multilateral net settlement obligation of any single participant in the system. The central bank commitment helps to further ensure that the LVTS will settle under all circumstances. Additionally, a participant may use either Tranche to send payment instructions, subject to applicable bilateral and multilateral net debit limits.[7] Currently, there are 17 participants in the LVTS (status July 2019, see website Payments Canada including domestic and international financial intermediaries. There is a large level of concentration in which the largest six LVTS participants are typically responsible for over 90 per cent of daily LVTS transfer value. The smallest five banks are only responsible for 1% of the turnover and less than 1% of the transactions. This means that the participants in LVTS are highly heterogeneous.

[7] Arjani and McVanel (2006) for a more in-depth discussion of the LVTS model.

2.2 Transaction data

We have transaction data available of Tranche 1 and 2 from 2002 until 2018. For each transaction we have used the settlement date, settlement time, sending and receiving participant, and amount. The number of participants varies from 14 in 2002 to 17 in 2018.

The data has been cleaned for the following transactions. First, we only keep transactions between 8.00 AM to 6.00 PM EST. These are the normal opening hours in which banks are active. LVTS is also open besides these times, but activity is normally limited. During the night, for example, the payments to CLS are made.[8] CLS payments are highly urgent payments but are very limited in number. Second, we removed all outgoing transactions from the central bank as we are interested in outages of commercial banks only. Payments from a participant to the central banks remain in the sample as this constitutes payment activity of a commercial bank (participant). Third, we remove all Canadian public holidays from the transaction data set. At most public holidays the system will be closed, which means there will be no payments exicuted at all in the system. There are also 'regional' public holidays in which the system is open, but the activity can be much lower than usual. Also activity around US public holidays may slow. This may cause false positives in which outages are detected by our algorithm, but in fact it is just a normal 'slow' day. Some LVTS participants are foreign bank branches or foreign subsidiaries operating in Canada, and thus have their headquarters outside Canada, e.g. in France, United Kingdom or the United States. For these, participants we also remove the transactions of the days in which the country of the headquarter has a public holiday.

Figure 1 gives insight to the number of transactions settled in LVTS. Figure 1a shows that the monthly daily average number of transactions has increased from roughly 26000 to 36000 between 2012 and 2018. This increase is mainly the result of the larger banks increasing their activity in LVTS. Figure 1b shows the percentage share of the transactions settled in a given hour. All transactions belonging to '8' are the transactions settled be-

[8] CLS stands for continuous linked settlement and takes care of foreign exchange transactions and operates between many different time zones.

tween 8.00 AM and 9 AM, etc. It is clear from this figure that the number of transactions in the last two hours are the lowest of the day time. Especially the last hour (between 5.00 PM and 6.00 PM) has a very low transaction volume. This is mainly due to the fact that banks mainly use this hour to make sure they have sufficient liquidity available in their account by the system closing time.

2.3 Reported operational outages

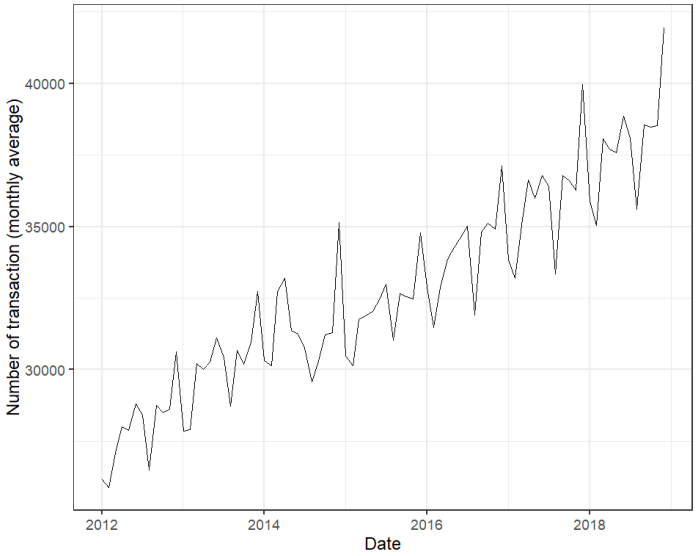
Besides LVTS transaction data, we have list of reported operational outages of LVTS' participants. This list states the participants that were unable to make any payments (severity 1 outage) and only a few transactions (severity 2 outage) for the years 2016 and 2017. Besides the participant name and severity type, the list contains the date, the start and end time of the incident . This list contains reported outages in which the participants where not able to make any payments (Severity 1) or only a few transactions (Severity 2). The total number of reported outages in 2016 and 2017 were 23 (16 severity 1 and 7 severity 2) and 26 (19 severity 1 and 7 severity 2), respectively. We have only included outages that took place during 8 AM and 6 PM. The average outage durations in those years 02:05 and 02:25 hours, respectively. The longest operational problem recorded was 12:40 hours in 2016 and 12:46 hours in 2017.

2.4 Special arrangements or features

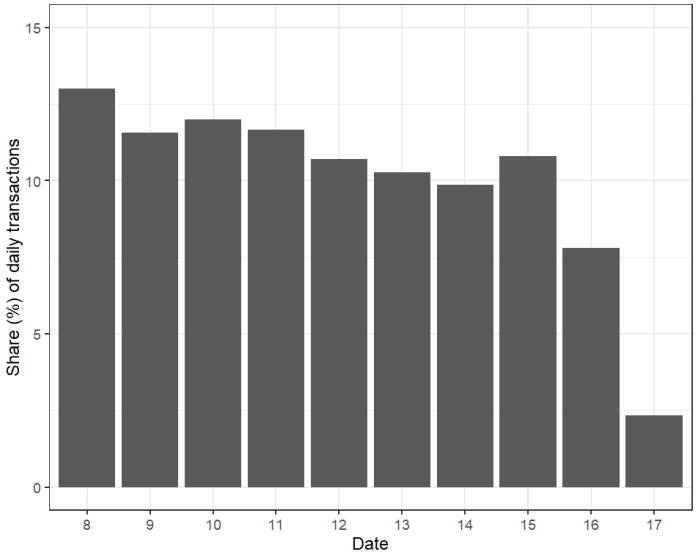
Procedures to follow in the case of an operational outage are governed by LVTS Rule 12. Rule 12 and accompanying procedures distinguish between types of outages. A Severity 1 outage occurs when a participant is unable to send/receive any payments via the LVTS. A Severity 2 outage is when the participant is able to send payments, however not at a normal processing pace; its normal payment processing operations are still disrupted. For Severity 1 and Severity 2 outages, section 12.14 of Rule 12 indicates that, if a participant encounters a technical, site or external problem (e.g., SWIFT connection problem, payments environment problem, site problem, or weather or civil problem) that may impact its abil-

Figure 1: The number of transaction in LVTS between 2012 and 2018.

(a) Monthly daily averages.



(b) Hourly averages.



ity to send or receive LVTS payment messages, the participant must notify the LVTS Help Desk within 15 minutes of becoming aware of the problem, identifying itself, the nature of the problem, and, if possible, the expected time by which the situation will be resolved. In the case of time-sensitive payments or given risk of a material liquidity trap, contingency procedures are available to mitigate risk of further disruption to other participants and FMIs. For instance, if a Participant is experiencing a Severity 1 Incident and cannot send payment messages via its SWIFT interface because of a technical, site or external problem that results in trapped liquidity or the inability of that Participant to meet critical time-sensitive obligations (e.g. CLS pay-ins, funding for ACSS settlement, and CDSX settlement), the Participant may use the Direct Network to send Payment Messages in accordance with the procedures contained within Rule 12. Note that the Direct Network can only be used to foster interbank transfers (SWIFT MT 205 messages).[9]

3 The algorithm

In line with Glowka et al. (2018), we also look at two different types of potential outages. First, if there are no transactions at all in a certain five minute time interval, this interval be referred to as "no payment activity (NoPa).[10] Second, if activity is much lower than usual (e.g. below 1 percentile) meaning having only a very limited amount of transactions. These types of intervals will be referred to as "low payment activity (LowPA)". The reasoning for looking at periods with lower transaction volumes is that financial institutions have a manual contingency procedure in which they can still process a limited amount of very urgent payments. This way, we can also limit the capacity for false negatives as these periods with low activity should be potentially be seen as outages but will not be picked up by the NoPA method.

[9] SWIFT message type 205 is often referred to as 202 in other jurisdictions.

[10] They look at intervals of 10 minutes, being one-third of the length of an outage that should be reported by a participant in TARGET2. In the LVTS, participants must inform Payments Canada within 15 minutes of encountering a disruption. Therefore, we look at 5 minute intervals, also being one-third of the minimum reported interval length. However, this period can be set to any desired value by the operator.

In contrast to Glowka et al. (2018), we do not have to exclude the extremely small participants. LVTS only has 17 participants. In contrast, TARGET2 has approximately 1000 direct participants of which many very small ones in terms of payment activity. However, the difference in activity is also quite large between the largest and smallest participants in LVTS.

If our algorithm would see a period from a small participant as low or no activity does not necessarily mean that a participant indeed faced a technical outage. It could be the result of not having any payment obligations to settle for some time or it may even delay intentionally (without having technical problems). Besides, we are not be able to prove in real-time that there was an outage with the available data. Our algorithm is intended to inform the payment operator that a participant has low or no activity for for example 15 minutes. In case it would take too long form the operator's perspective it can contact the participant to see what is going on. Lastly, participants only have to report to the operator when they have had a technical outage of at least 15 minutes, which is three consecutive intervals.

3.1 No payment activity

The no payment activity algorithm (NoPA) identifies periods a participant has not sent in any payment instruction into the LVTS. We look at intervals with no transactions of 5 minutes.

$$NoPA = \begin{cases} yes, \text{if} \quad TNR_{fi,t} = 0 \\ no, \text{if} \quad TNR_{fi,t} > 0 \end{cases} \tag{1}$$

where $TNR_{fi,t}$ is the number of transactions a financial institution fi has at five minute time interval t.

Figure 2 illustrates the absolute (2a and 2b) and relative (2c and 2d) number of 5 minute periods without transactions for all banks (2a and 2c) and the largest five banks (2b and

2d) in LVTS, respectively.[11]

Figure 2c shows that the number of five minute periods without transactions is just below 50%. The reason for so many periods without any transactions is that quite a few banks are not very active in the system throughout the whole day. These banks have periods in which they do not send in any payments. If we zoom in to the five largest financial institutions, which tend to be the most active banks, this number decreases to below 20%, see Figure 2d. The number of periods without transactions decrease over the years to close to 15%. This is still a relatively large number as 1 in 5 to 6 periods of five minutes there are no transactions.

3.2 Low payment outages

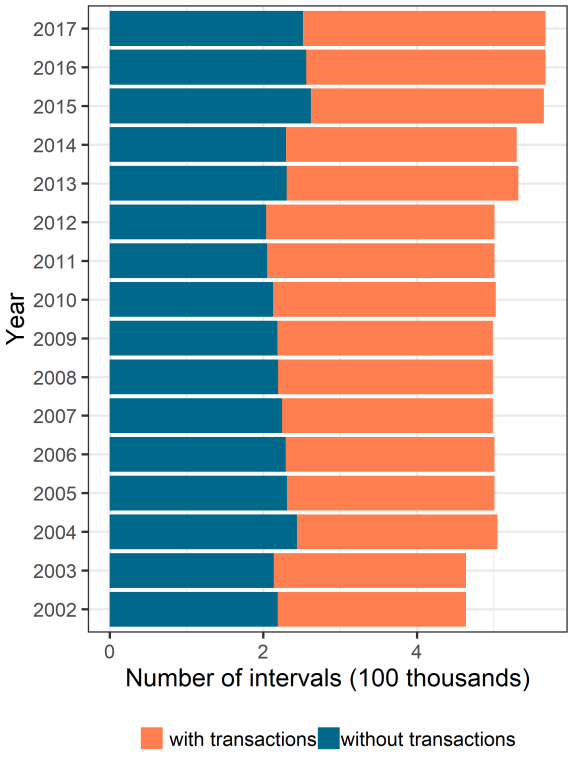
In contrast to the NoPA outage setup we accept very few payments to be sent in to the LVTS in the low payment activity (LowPA) setup. We base this low activity on the behaviour of the individual participant. Low activity is defined as the number of transactions settled in a given 5 minute interval over the whole data sample below 1 percentile. We zoom into the payment behaviour of that respective participant at that respective time interval. First, participants often send in more payment instructions at given times e.g. early in the morning and in the afternoon and have fewer payments at other times, see e.g. Massarenti et al. (2012) or Heijmans and Heuver (2014). Second, we would like to exclude periods of no activity in the case that is 'normal' for that participant to have no or low activity. To be able to look at unusually low payment activity we must correct for this natural difference in payment activity at the participant level.

$$\frac{TNR_{fi,t}}{\overline{TNR_{fi,t,y}}} < 1\,percentile \tag{2a}$$

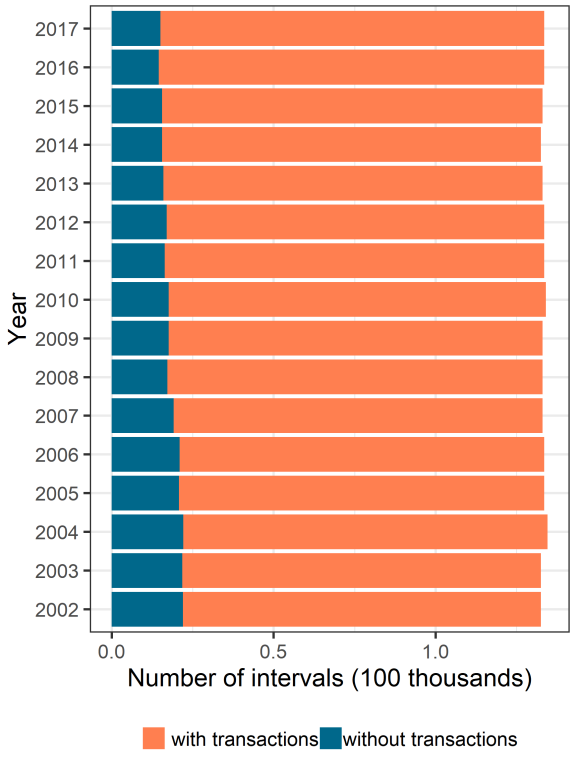
[11] As the number of financial institution increased from 14 in 2002 to 17 in 2017, the absolute number of five minute intervals of all the financial institutions increased accordingly. As the number of business days varies per year, the total number of 5 minutes intervals also varies.

Figure 2: Five minute intervals with and without transactions.

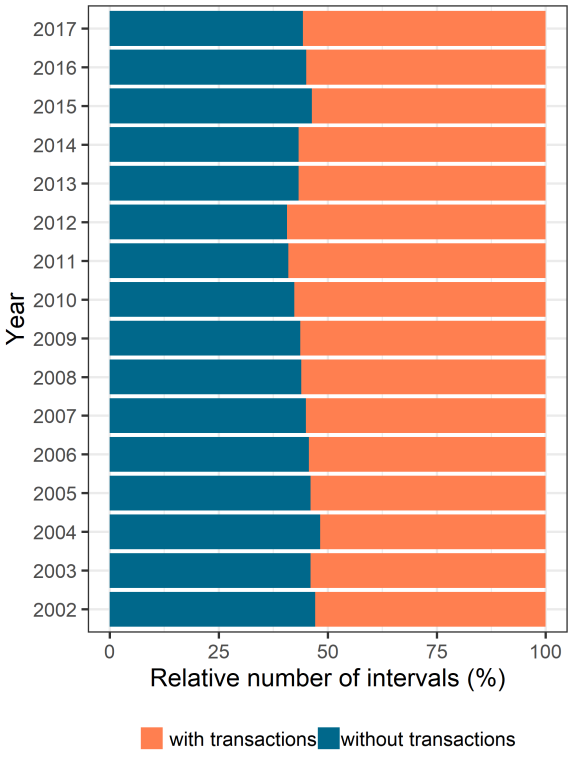
(a) Absolute number all banks.



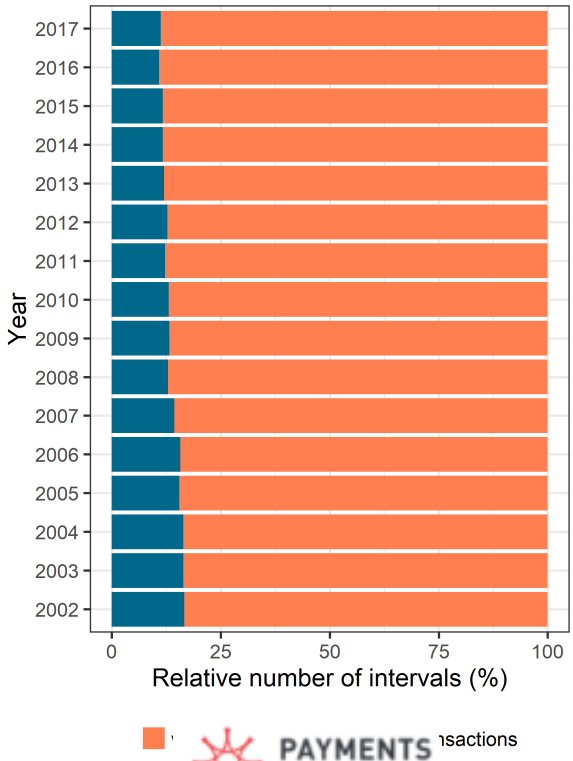
(b) Absolute five largest banks.



(c) Relative share all banks.



(d) Relative share five largest banks.



$$TNR_{fi,t} > 5 \tag{2b}$$

where $TNR_{fi,t}$ is again the number of transactions a participant fi has at five minute time interval t, $\overline{TNR_{fi,t,y}}$ is the mean number of transactions of participant fi at five minute interval t over the year y. The $\overline{TNR_{fi,t,y}}$ is the mean per year as the numbers may change over the years.

In our model setup of LowPA, it is considered an outage if the payment activity is below the 1 percentile of that respective participant and time interval (equation 2a) and a minimum of 5 transactions have been sent in (equation 2b).

4 Results

This section describes the outcome of our outage detection method compared to the reported outages. Section 4.1 shows the detected outages for the period ranging from 2002 to 2017. Section 4.2 describes the day of the week and intraday patterns of the outages. In contrast with Glowka et al. (2018) we have a list of reported outage events by the participants. This allows us for checking whether participants do indeed report their outages, see section 4.3. These reported outages presents an opportunity to assess the validity of our model and empirical likelihood of false positives. There may be an incentive for participants to not report their operational outage. First, as per the LVTS Rules, participants need to have an up time of at least 98% during each calendar month. Every time they report an outage their up time decreases. Second, they do not want to be known by the operator (and their peers) as a bad performer in terms of their technical infrastructure.

4.1 Detected outages by the NoPA and LowPA algorithm

Figure 3 shows the number of outage intervals (1 to 4) for the NoPA and LowPA model for all banks and the largest five banks. As expected, the number of outages decreases going

from one to four intervals. As Glowka et al. (2018) state, the longer the outage intervals the less likely it is that it is just a coincidence.

Figure 3a and 3a show the outages for the differentiated model with low activity. The number of outages found by this model setup for the largest five banks in the system is close to the outages found by all banks (including the largest five banks). The reason for this is that only outages are included if the number of transactions found is lower than the 1 percentile. For some of the smaller banks the 1 percentile is equal to zero transactions. As lower than zero transactions is not possible, these periods will not be picked up by this second algorithm (but will be picked up under the first algorithm).

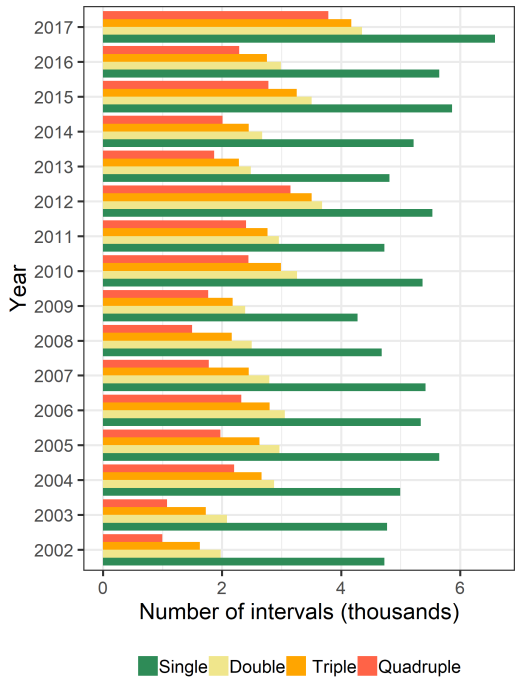
4.2 Outages at day of the week and intraday

Figure 4 shows the number of outages (4 consecutive 5 minute periods) found by the LPA algorithm differentiated to the day of the week. We use four consecutive intervals to be beyond the reporting obligation time interval of 15 minutes. The figure clearly shows that on Monday there are more potential outages detected than in the rest of the week combined. According to the system operator, this can be explained by the fact that software updates, new releases of the LVTS system and the participant's internal systems are mainly introduced over the weekend. These problems are usually solved the same day the system as the software updates or changes are released. As the number of detected outages on Tuesday is much smaller than on the Monday and in line with the rest of the week, this seems plausible.

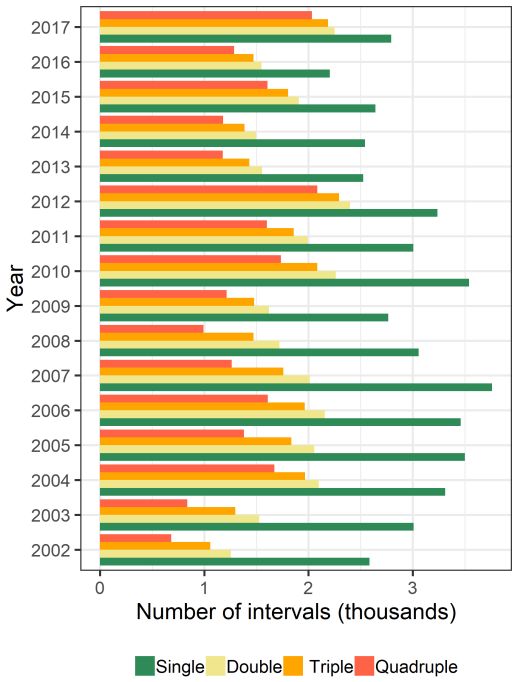
Figure 5 depicts the outages find by the LPA model by hour of the day. The last two hours of the day ranging from 16.00 to 18.00 hours have many more outages found. The participants in this period typically use to make sure that their end of day balance is adequate resulting in payments which are relatively high in value but low in number. The other hours of the day do not show a large variation.

Figure 3: The number of single, double, triple and quadruple intervals without transactions in a row.

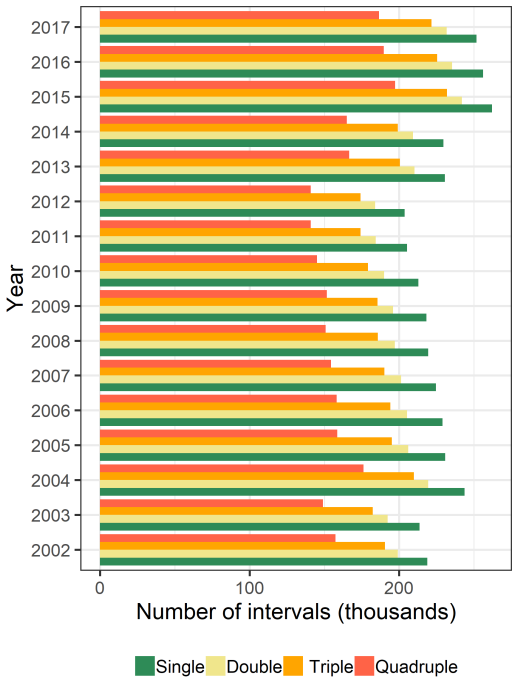
(a) LowPA all banks.



(b) LowPA five largest banks.



(c) NoPA all banks.



(d) NoPA five large banks.

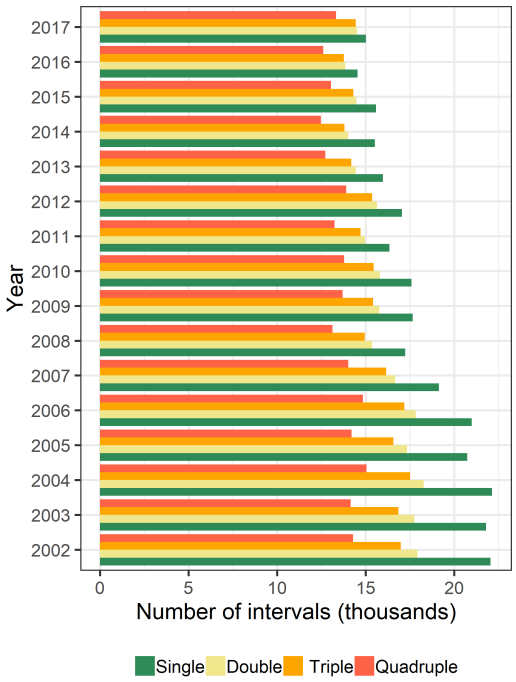
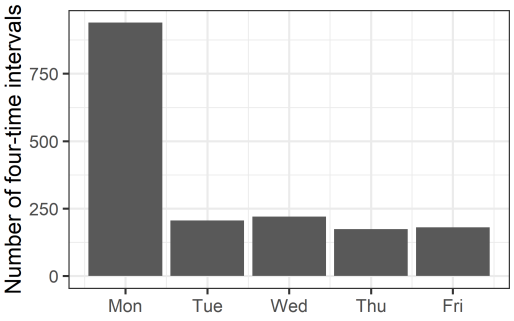


Figure 4: Outages found by LowPA algorithm by day of the week.

(a) all banks



(b) 5 large banks

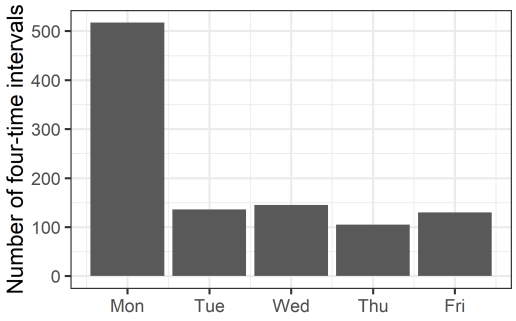
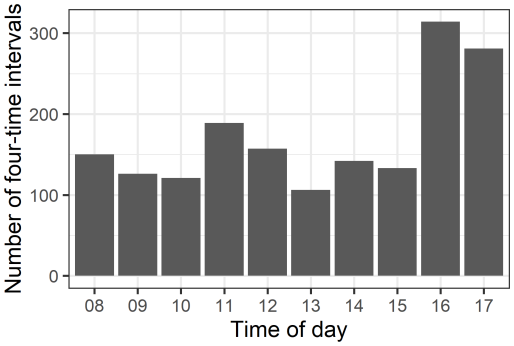
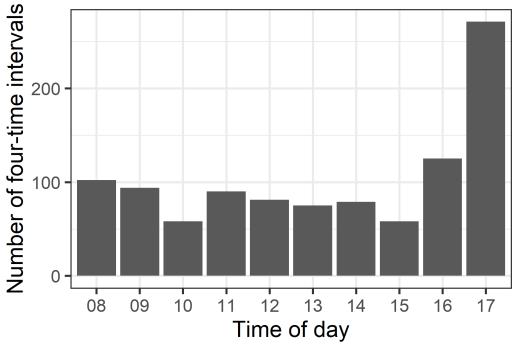


Figure 5: Outages by LowPA algorithm by hour of the day.

(a) all banks



(b) 5 large banks



4.3 Validation of the algorithm: detected versus reported outages

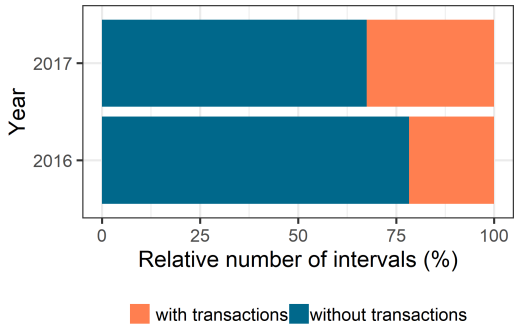
We now move to the list with reported outages by the participants, see section 2.3. We check whether the algorithm picks up those periods as outages, which is basically a check on the false negative error. To check the algorithm we only inlcude 1) those participants with a reported outage and the 2) time interval of the reported outage. The time interval has to be within 8.00 AM and 18.00 PM as this is the time range we investigate the data. As the algorithm works best for the largest five participants in the system, we focus on those in this section.

Figure 6 shows the relative number of periods with and without transactions for the largest 5 banks. During 75% of the reported outage periods, there are no transactions detected at all. In the other 25% of the periods there have been payments detected. Most of these payments are related to the severity 2 incidents in which participants are still able to make some payments. The number of payments is still higher than the 1 percentile and therefore not excluded by the algorithm. Ideally, you may want to pick up these severity outage by our algorithm. However, in case of a severity 2 error the operator is aware of the problem. Therefore, in that case the operator does not have to be informed by the algorithm anymore. Some of the payments are within the same five minute interval investigated but (just) before the outage started. This means that if the outage started at 10.04 AM and there has been made a few payments between 10.00-10.03 AM the five minute interval (10.00-10.05 AM) counts towards the intervals with transactions.

Figure 7 shows the number of periods in a row with low (7a) and no payment activity (7b) for the periods of reported outages for the large five banks. The number of outage interval without transactions is much larger than with transactions. From Figure 7b we can see that the number of four consecutive periods with outages is almost the same as the one period outage. As all except one outage was longer than three five minute intervals we can state that all reported outages are picked up by the algorithm.

Looking at the LowPA output (7a) we see that is a few cases where there is still some activity wehn they report an outage. Some of these detected time intervals with a low number of

Figure 6: Periods of reported outages only by the large five banks.

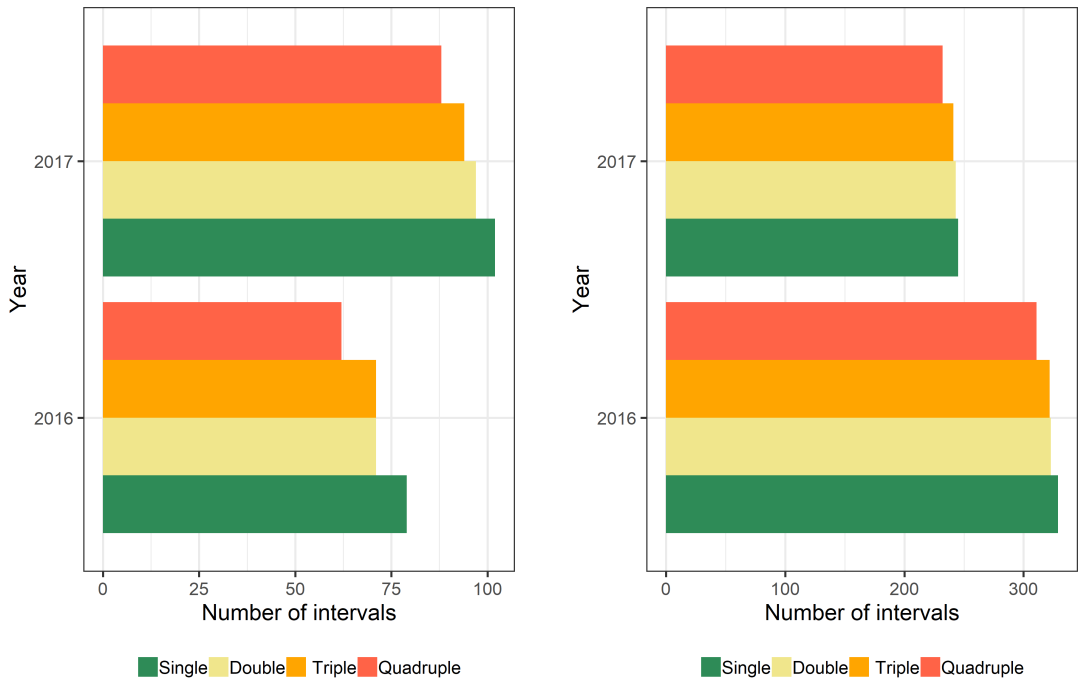


transactions will be the beginning or the end of the outages with no transactions at all. In case there are four consecutive periods with low activity, we can assume that this is linked to Type2severity outages.

Figure 7: The number of single, double, triple and quadruple outage intervals.

(a) LowPA 5 large banks

(b) NoPA 5 large banks



5 Conclusions

This paper developed an algorithm to detect potential operational outages at individual participants in LVTS. We distinguish two different setups of the algorithm. First, we identify periods in which no payments are made at all by a participant. As a bank who is not able to send in payment instructions will become visible in the data if for a certain period of time no payments have been observed. Second, we identify periods in which there is an unusual low number of payment instructions sent in by the participant. The rationale behind this second set up is that a bank that is not able to send in payments the normal way may have a back up functionality for very urgent payments. The results show that in roughly 50% of the five minute periods, a participant does not send in any payments. Zooming in to the largest five financial institutions, this percentage decreases to less than 20%. As expected, the number of consecutive periods of five minutes decrease going from 1 (five minutes) to 4 (20 minutes) periods. However, for the large five participants, this decrease is much lower than for all participants. Large banks basically have payments in most five minute intervals and, therefore, it is unlikely that they do not have at least some payments in two or three consecutive periods. When these large financial institutions have more than one period without payments, this is more likely due to a technicial problem. These problems may take a bit of time to resolve (more than 20 minutes).

Most of the outages detected are on Monday. This is due to the fact that new releases and software updates are usually done over the weekend when the system is closed. Problems with the new functionality or software updates will therefore be on Mondays. These problems are usually solved the same day and participants can send in payment instructions normally again. Reported operational outages by the participants to the operator show that our algorithm picks up these outages. During the reported outages the participants were not able to make any payments for the most. In the minority of cases the participants were still able to send in some payments.

Overall, we can conclude that our algorithm works well for the large five banks. As the

small banks do not send in enough payments during the day and have too mamy consecutive periods with no payment activity it will lead to too many false posivites or negatives. This is not a reduction of the usefulness of our algorithm, but the algorithm works much better for large (active) participants than for small (less active) participants. At the same time, due to the low activity the impact of is also very limited as other participants do not expect to receive large sums of liquidity from this small participant.

In order to implement a "real time potential outage detection method" as a monitoring tool for the payment operator, it is crucial to have real-time data. The method provided in this paper will only be able to detect potential outages, not predict them at this stage. As this type of algorithm will have false positives (and negatives), a potential outage detected by the algorithm does not mean that the respective participant has a technical outage with 100% certainty. The participant may not have payment instructions that have to be made or it may be delaying payments intentionally. Therefore, it is advisable to also look at payment delay indicators to check whether a participant is potentially delaying its payments. In case the operator gets a signal of a participant having low or no activity for some number of intervals, the appropriate follow up would be to contact the respective participant to see what the problem may be.

References

Abbink, K., Bosman, R., Heijmans, R., and van Winden, F. (2017). Disruptions in large value payment systems: An experimental approach. *International Journal of Central Banking*, 13(4):63–95.

Arjani, N. and McVanel, D. (2006). A primer on canada's large value transfer system. *Bank of Canada*.

Bech, M. and Garratt, R. (2003). The intraday liquidity management game. *Journal of Economic Theory*, 109:198–210.

Bech, M. and Garratt, R. (2006). Illiquidity in the interbank payment system following wide-scale disruptions. *Federal Reserve Bank of New York Staff Reports*, 239.

Bech, M. and Hobijn, B. (2007). Technology diffusion within central banking: The case of real-time gross settlement. *International Journal of Central Banking*.

Benos, E. and, G. R. and Zimmerman, P. (2012). Bank behaviour and risks in chaps following the collapse of lehman brothers. *Bank of England Working Paper*, (451).

Berndsen, R. and Heijmans, R. (2020). Risk indicators for financial market infrastructures: From high frequency transaction data to a traffic light signal. *DNB Working Paper*, 557:forthcoming.

Clarke, A. and Hanckock, J. (2013). Payment system design and participant operational disruptions. *Journal of Financial Market Infrastructures*.

CPSS (2012). Principles for financial market infrastructures: Disclosure framework and assessment methodology. *Bank for International Settlements*.

Diehl, M. (2013). Measuring free riding in large-value payment systems: The case of TARGET2. *Journal of Financial Market Infrastructures*, 1(3):31–53.

Diehl, M. and Müller (2015). Analysis of the use and impact of limits. In Laine, T., editor, *Quantitative Analysis of Financial Market Infrastructures: Further Perspectives on Financial s Stability*, volume E:50, pages 14–42. Bank of Finland.

Glowka, M., Paulick, J., and Schultze, I. (2018). The absence of evidence and the evidence of absence: an algorithmic approach for identifying operational outages in target2. *Journal of Financial Market Infrastructures*, 6(2/3):63–91.

Heemeijer, P. and Heijmans, R. (2015). Central bank intervention in large value payment systems: An experimental approach. *Journal of Financial Market Infrastructures*, 3(3):17–49.

Heijmans, R. and Heuver, R. (2014). Is this bank ill? the diagnosis of doctor TARGET2. *Journal of Financial Market Infrastructures*, 2(3):3–36.

Kaliontzoglou, A. and Müller, A. (2015). Implementation aspects of indicators related to payments timing. In Diehl, M., Alexandrova-Kabadjova, B., Heuver, R., and Martinez-Jaramillo, S., editors, *Analyzing the Economics of Financial Market Infrastructures*, pages 169–190.

Klee, E. (2010). Operational outages and aggregate uncertainty in the federal funds market. *Journal of Banking and Finance*, 34(10):2386–2402.

Massarenti, M., Petriconi, S., and Lindner, J. (2012). Intraday patterns and timing of TARGET2 interbank payments. *Journal of Financial Market Infrastructures*, 1(2):3–24.

Triepels, R., Daniels, H., and Heijmans, R. (2018). Detection and explanation of anomalous payment behaviour in real-time gross settlement systems. In *Enterprise Information Systems. ICEIS 2017. Lecture Notes in Business Information Processing*, volume 321. Springer, Cham.