



The Electronic Vote in Venezuela

Technical evaluation of an electoral process

The 15th-August-2004 Presidential Recall Referendum as a study case





- **Aims**
- **Outline of the electoral system**
- **Conditions established by CNE**
- **Findings in telecommunications**
- **Conclusions and recommendations**



- Outline of the Venezuelan automated electoral system.
- Demonstration of the anomalous behavior of the automated electoral system during the Presidential Recall Referendum 15August2004; correlation between technological and electoral variables.
- Conclusions and recommendations



The electoral system is composed of three subsystems with clearly defined functions :

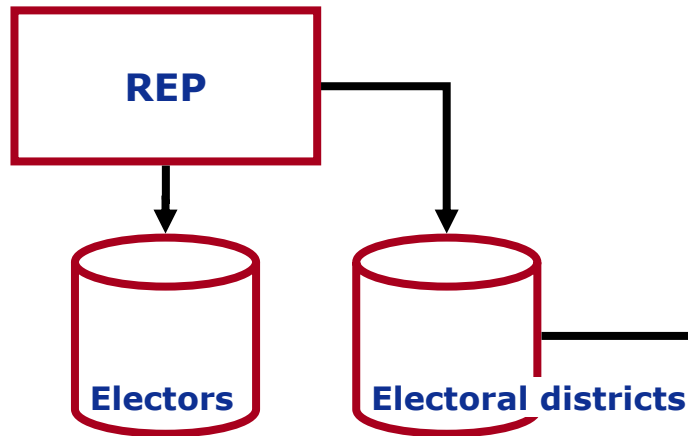
- **Permanent electoral registry (REP):** basic information on the electors and electoral districts.
- **Pre-electoral subsystem (nominations and positions):** it maintains a registry of the different electoral events, positions in dispute and candidates.
- **Voting-Counting-Totalizing:** it includes the manual and automated balloting procedures. In voting tables: counting of votes and emission of tally reports (*actas*). In electoral boards: regional or national summing up of tally reports and emission of results.

88,7% of PRR 2004 votes were cast electronically through touch screen machines, amounting to 8.6 MM votes out of a total of 9,85 MM

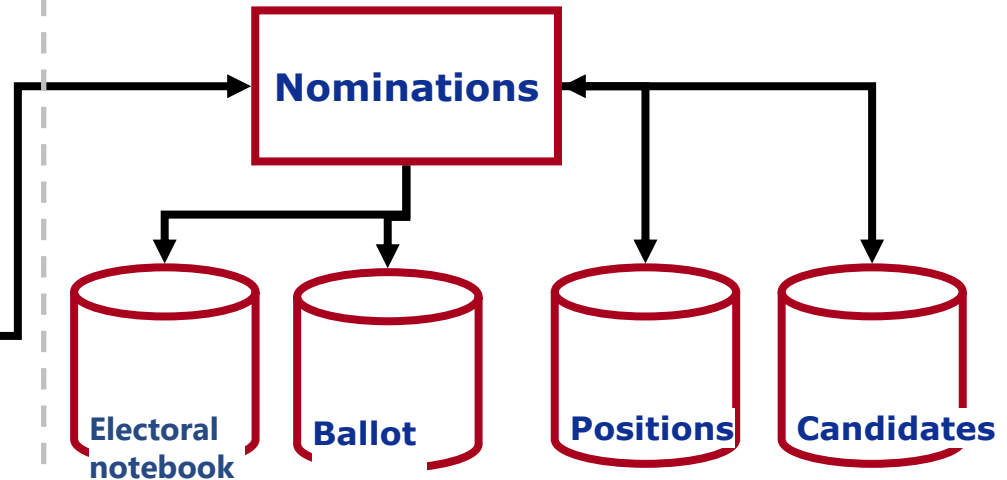
Electoral System Outline - (cont.)



Permanent Electoral Registry

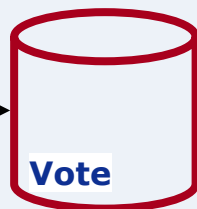


Pre-electoral

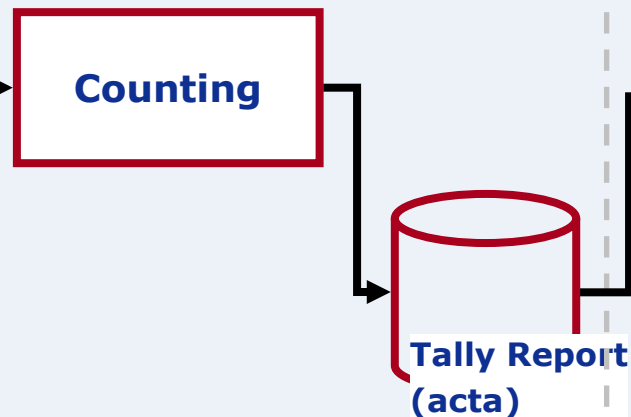


Voting

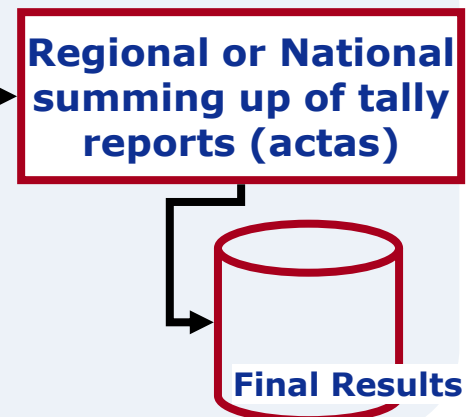
Voter
+
Paper or electronic Ballot



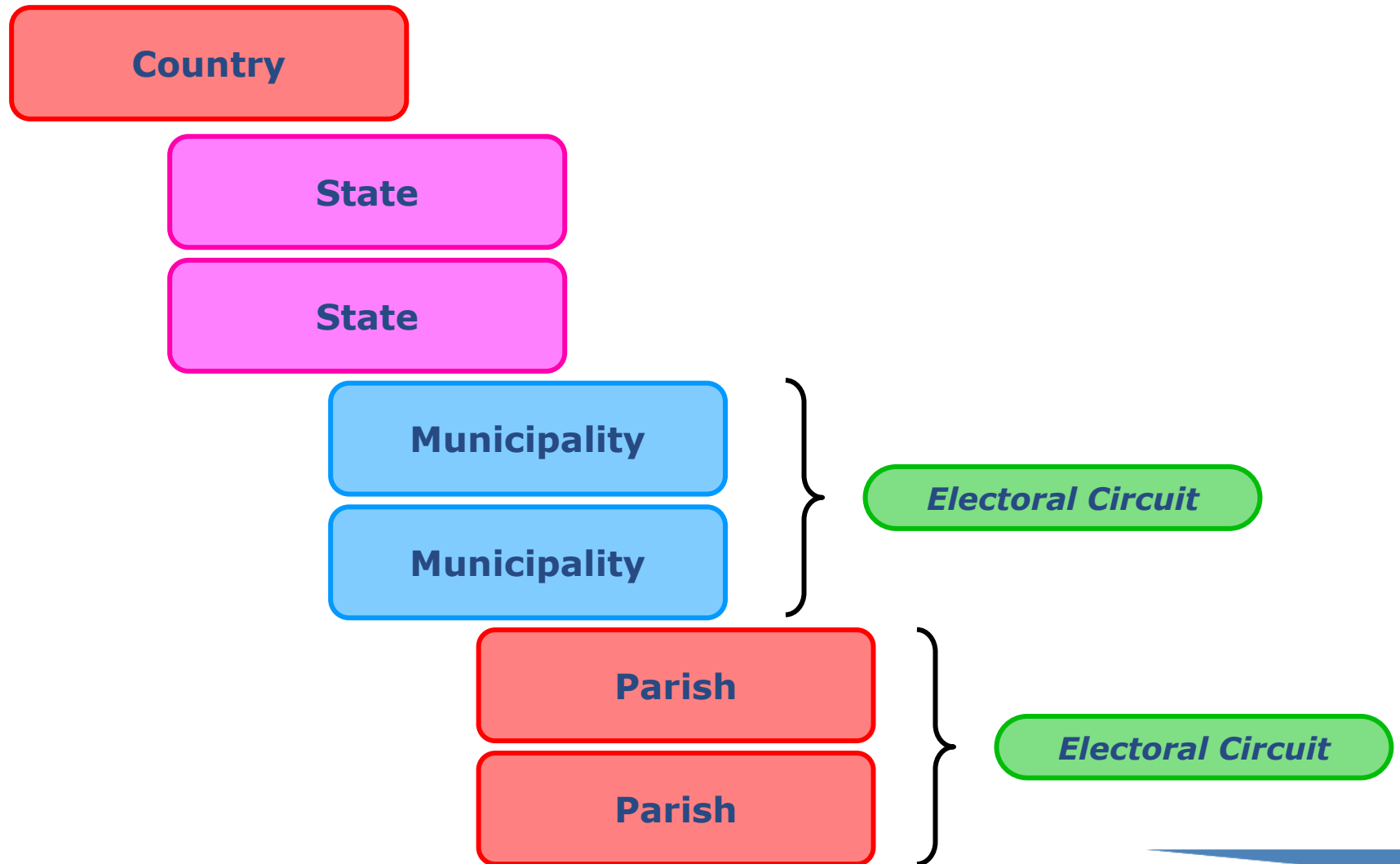
Vote Counting



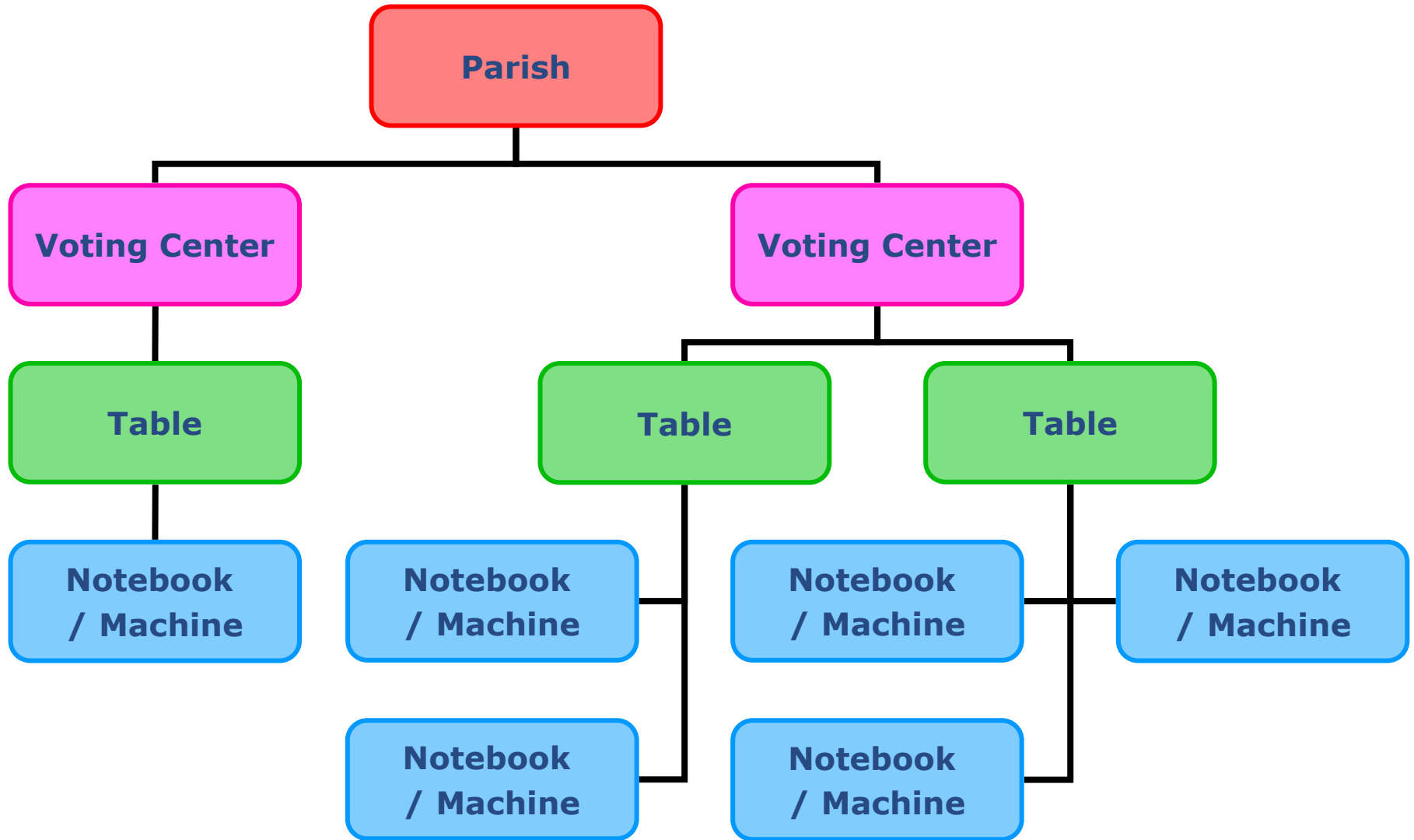
Totalizing



Venezuelan Political Organization



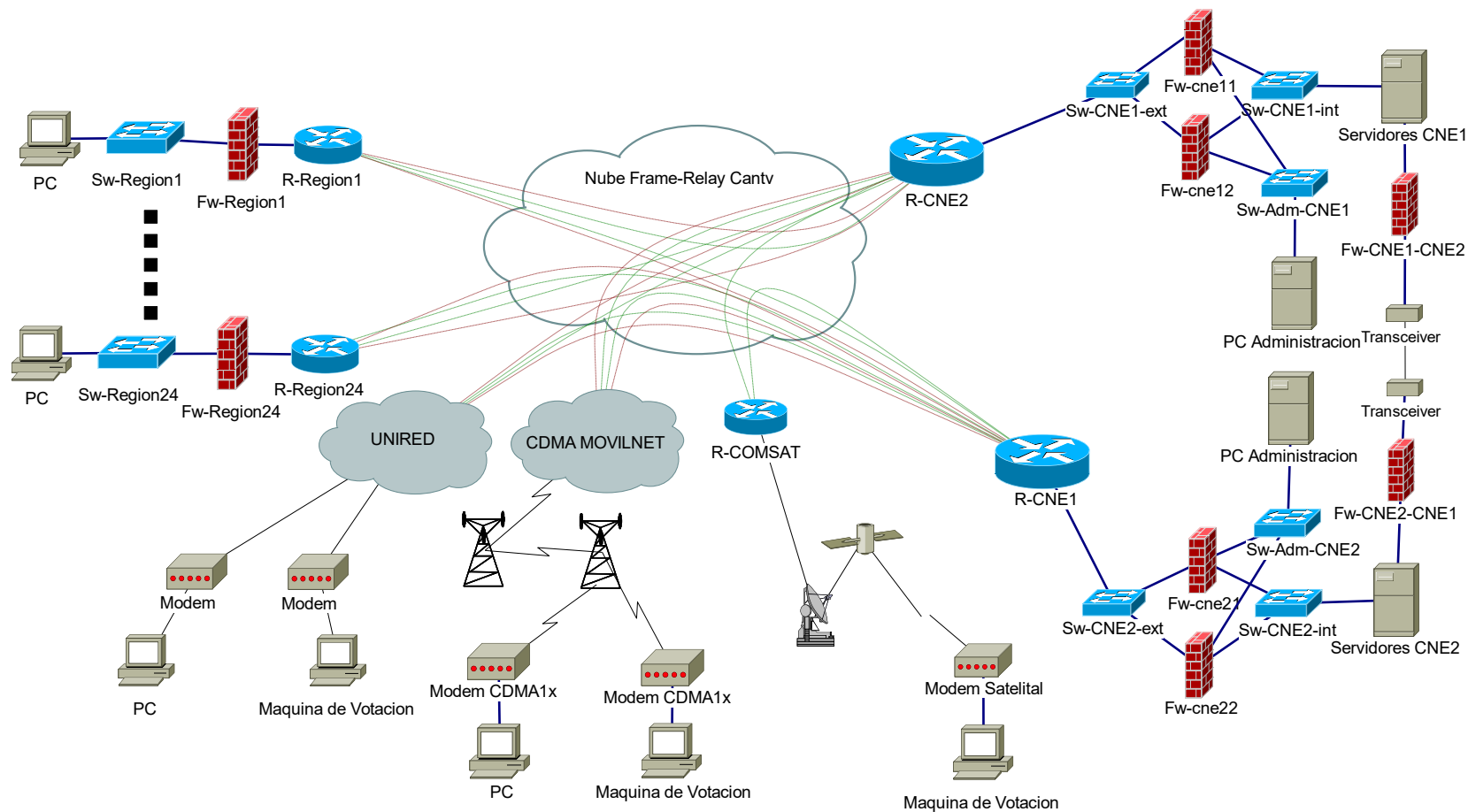
Electoral Organization



Data Network Topology



PROYECTO ELECCIONES CNE 2004





- **All voting machines must be identical:**

- ✓ They have the same hardware, without internal wireless communication devices.
- ✓ They work under the same operating system. It must be configured in the same way.
- ✓ They execute the same votes recording and counting software, except for those data intrinsically tied to the identification of the machine such as: voting center, table and electoral notebook code numbers to which it is assigned, as well as the number of allowed electors.



- **The machines transmit information on tally reports (actas) to central CNE servers .**

The tally reports (actas) have the same structure, that is to say contain the same volume of information, which is independent of the values of the electoral variables associated with it, like : voting center, table and electoral notebook code numbers, geographic location codes, polling opening and closing times, number of voters, number of absentees and result of the event.

Example - Hypothetical Voting Results



Voting Center	Table	Note-book	Opening Time	Closing Time	ELECTORS	Actual VOTERS	YES VOTES	NO VOTES	NULL VOTES
98765	4	3	15/08/2004 07:15:41AM	16/08/2004 01:05:30AM	45	40	20	15	5
100	1	1	15/08/2004 06:00:11AM	16/08/2004 12:00:10AM	120	110	55	55	0
12345	2	2	15/08/2004 6:40:20AM	16/08/2004 12:45:00AM	260	245	100	135	10
441	3	1	15/08/2004 06:02:00A M	16/08/2004 10:15:30pM	450	400	195	200	5
77788	4	3	15/08/2004 07:20:00A M	16/08/2004 06:32:03PM	500	420	250	240	30
55	1	1	15/08/2004 06:00:20A M	15/08/2004 11:55:09PM	600	580	320	160	0

Example - Individual Votes Memory Storing



<i>Vote Value</i>	<i>Vote Serial Number.</i>												<i>Amount of Bytes</i>
		<i>Vote</i>	<i>Serial Number</i>										
NO	123000451	N	1	2	3	0	0	0	4	5	1		10 bytes
YES	123000452	Y	1	2	3	0	0	0	4	5	2		10 bytes
YES	123000453	Y	1	2	3	0	0	0	4	5	3		10 bytes
YES	123000454	Y	1	2	3	0	0	0	4	5	4		10 bytes
NO	123000455	N	1	2	3	0	0	0	4	5	5		10 bytes
NO	123000456	N	1	2	3	0	0	0	4	5	6		10 bytes
YES	123000457	Y	1	2	3	0	0	0	4	5	7		10 bytes

10 bytes per vote

This is a simplified example where to each vote a serial number is assigned. Data are stored in an encrypted way. Theoretically, once serial numbers and 'yes' or 'no' votes are encrypted, they cannot be deciphered to know the sequence. But, this is not so accurate since the process is reversible and would allow for a violation of the secrecy of vote.

Example – Tally (Actas) Storing in Memory



Information in Tally Reports (Actas)

Electronic information stored

Voting Center	98765
Table	4
Notebook	3
Opening Time	15/08/2004 07:15:41AM
Closing Time	16/08/2004 01:05:30AM
ELECTORS	45
Actual VOTERS	40
Yes VOTES	20
NoVOTES	15
Null VOTES	5

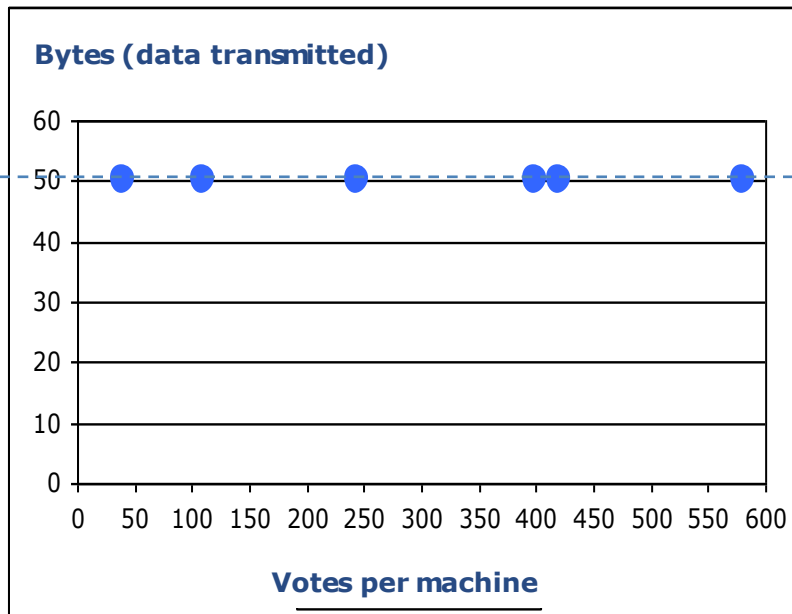
DATA														MEMORY SPACE		
9	8	7	6	5										5 bytes		
4														1 bytes		
3														1 bytes		
2	0	0	4	0	8	1	5	0	7	1	5	4	1		14 bytes	
2	0	0	4	0	8	1	6	0	1	0	5	3	0		14 bytes	
0	4	5												3 bytes		
0	4	0												3 bytes		
0	2	0												3 bytes		
0	1	5												3 bytes		
0	0	5												3 bytes		

Voting Center	55
Table	1
Notebook	1
Opening Time	15/08/2004 06:00:20AM
Closing Time	15/08/2004 11:55:09PM
ELECTORS	600
Actual VOTERS	580
Yes VOTES	320
NoVOTES	160
Null VOTES	0

0	0	0	5	5											5 bytes
1														1 bytes	
1														1 bytes	
2	0	0	4	0	8	1	5	0	6	0	0	2	0		14 bytes
2	0	0	4	0	8	1	5	2	3	5	5	0	9		14 bytes
6	0	0												3 bytes	
5	8	0												3 bytes	
3	2	0												3 bytes	
1	6	0												3 bytes	
0	0	0												3 bytes	

50 bytes partially (independent of electoral results)

Example – *EXPECTED* data transmission graph



● Represents a voting machine



Vote totals
transmission

Voting Center	Actual VOTERS
98765	40
100	110
12345	245
441	400
77788	420
55	580

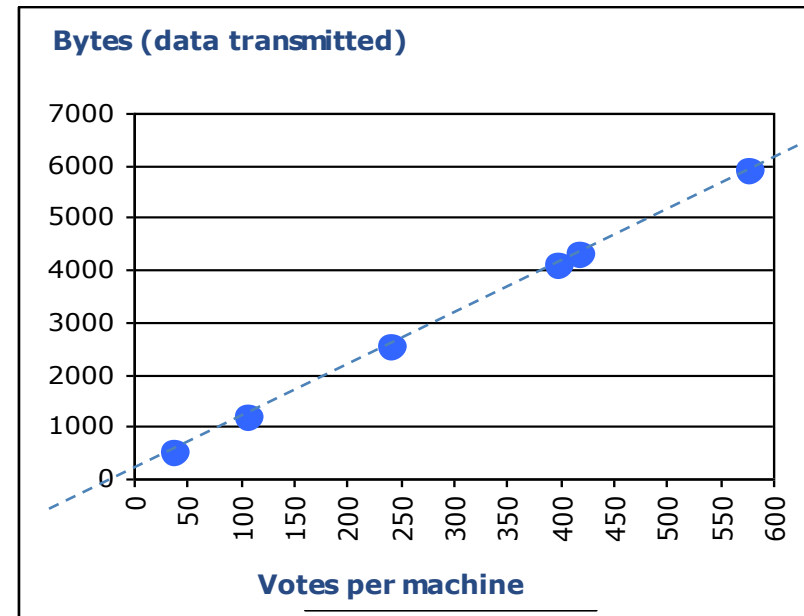
Example – **NOT EXPECTED** data transmission graph



Individual
votes

transmission

Voting Center	Actual VOTERS
98765	40
100	110
12345	245
441	400
77788	420
55	580



● Represents a voting machine



- The machines would print the results of the electronic vote counting *after* connecting themselves and transmitting data to the main CNE totalizing servers.
- Results were not due to be transmitted before the closing official time of the electoral event.

The initial closing time for the PRR event of the 15thAugust2004 was agreed for 16:00 hours. Soon it was delayed to 20:00 hours and finally, it was set to 00:00 hours of the 16thAugust2004.



- **Totalizing servers at CNE-1 and CNE-2 were identical** as far as the number and type of servers, their hardware, as well as their operative and electoral administration software.
- **Totalizing servers only had to transmit reception acknowledgement data back to voting machines.** It means that a small amount of bytes had to be transmitted back to voting machines in comparison to that sent by voting machines to servers, once a session was established successfully.



- **The transmission of results was in itself part of an automated and not human attended process that obeyed a prescribed source code.**

All data traffic had to be directed towards the main totalizing center, i.e. CNE-1. Only in the event of failure of main servers the contingency computer center (CNE-2) would start operating and directly be attending the voting machines.



- Since the machines are identical and transmit vote totals, it is expected that **the volumes of data in terms of bytes sent to totalizing servers are similar.**
- Since the totalizing servers only transmit information of recognition, authorization and acknowledgement towards the machines, it is expected that **the number of outgoing bytes from totalizing servers to machines was much smaller than that received from voting machines.**



- Being that the transmission of results is an automated process, **the termination of the sessions of communication between voting machines and totalizing servers must be a systematic action activated when the prescribed conditions of transmission are fulfilled.**

What it should had been demanded: in order to give greater guarantees on the integrity of the data stored in the machines, the transmission of results to central servers had to be made *after* the tally reports (actas) were printed and satisfactory manual public counting of votes was performed.



Findings in telecommunications



The present study is based on the following sources of information:

- Log of sessions established between voting machines and the CNE totalizing servers through the wire telephone network of CANTV.
- Log of sessions between the voting machines and the totalizing servers of the CNE through the cellular telephone network of Movilnet (CANTV subsidiary).
- Official results of the referendum of the 15th of August of 2004, published by the CNE.
- Contract closure report on the process of Presidential Recall Referendum of 15th of August 2004, produced by the supplier of telecommunications.
- Tally reports (actas) emitted by the voting machines during the 15th and 16th of August.

Sources of information – (cont.)



Wire telephone network – Part of *log* of sessions

Date	Acct-Output-Octets	Acct-Input-Octets	Acct-Terminate-Cause	Acct-Session-Id	User-Name	attribute-90	attribute-91
Sun, 15 Aug 2004 07:19:24	0	312	Lost Carrier	0035FC24	ZULIA_10@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 20:18:06	3.025	7.684	Lost Carrier	0036BAC0	ZULIA_20@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 20:34:27	7.528	13.366	Lost Carrier	0036BC4B	ZULIA_20@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 20:44:17	81	66	User Request	0036BDEB	ZULIA_20@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 21:11:01	4.526	9.371	Lost Carrier	0036C0CC	ZULIA_4@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 21:42:28	39.026	62.003	Lost Carrier	0036C22F	ZULIA_4@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 22:01:46	16.534	27.036	Lost Carrier	0036C569	ZULIA_4@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 22:14:24	7.528	13.099	Lost Carrier	0036C77B	ZULIA_13@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 22:21:01	1.524	0	User Request	0036C8B5	ZULIA_13@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 22:22:02	1.524	1.711	User Request	0036C8CC	ZULIA_13@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 22:25:55	3.083	7.248	Lost Carrier	0036C90F	ZULIA_13@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 22:27:01	7.775	134.487	Lost Carrier	000E90D1	LARA_4@cne2004.gov.ve	srv-aaa	CNE1
Sun, 15 Aug 2004 16:47:32	22	2.596	User Request	000E5163	36480_1_1_9@cne2004.gov.ve	srv-aaa	CNE1
Sun, 15 Aug 2004 16:52:07	212	2.616	Lost Carrier	0000D745	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 16:57:24	212	2.616	Host Request	0000D747	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:02:21	196	2.602	Lost Carrier	64385	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:07:21	212	2.616	Lost Carrier	0000D753	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:17:51	204	2.582	Lost Carrier	0000D758	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:23:08	180	2.588	Host Request	0000D75C	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:28:13	188	2.568	Lost Carrier	0000D760	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:33:10	180	2.588	Lost Carrier	0000D764	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:40:27	196	2.602	Host Request	0000D766	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:43:08	6.847	36.514	Lost Carrier	0000D76B	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:57:56	6.522	31.534	Lost Carrier	0000D771	46940_1_2_8@cne2004.gov.ve		
Sun, 15 Aug 2004 18:08:26	310	975	Lost Carrier	0004C4D4	21810_1_1_4@cne2004.gov.ve	srv-aaa	CNE1
Sun, 15 Aug 2004 18:11:40	5.265	12.557	Lost Carrier	0004C4D9	21810_1_1_4@cne2004.gov.ve	srv-aaa	CNE1



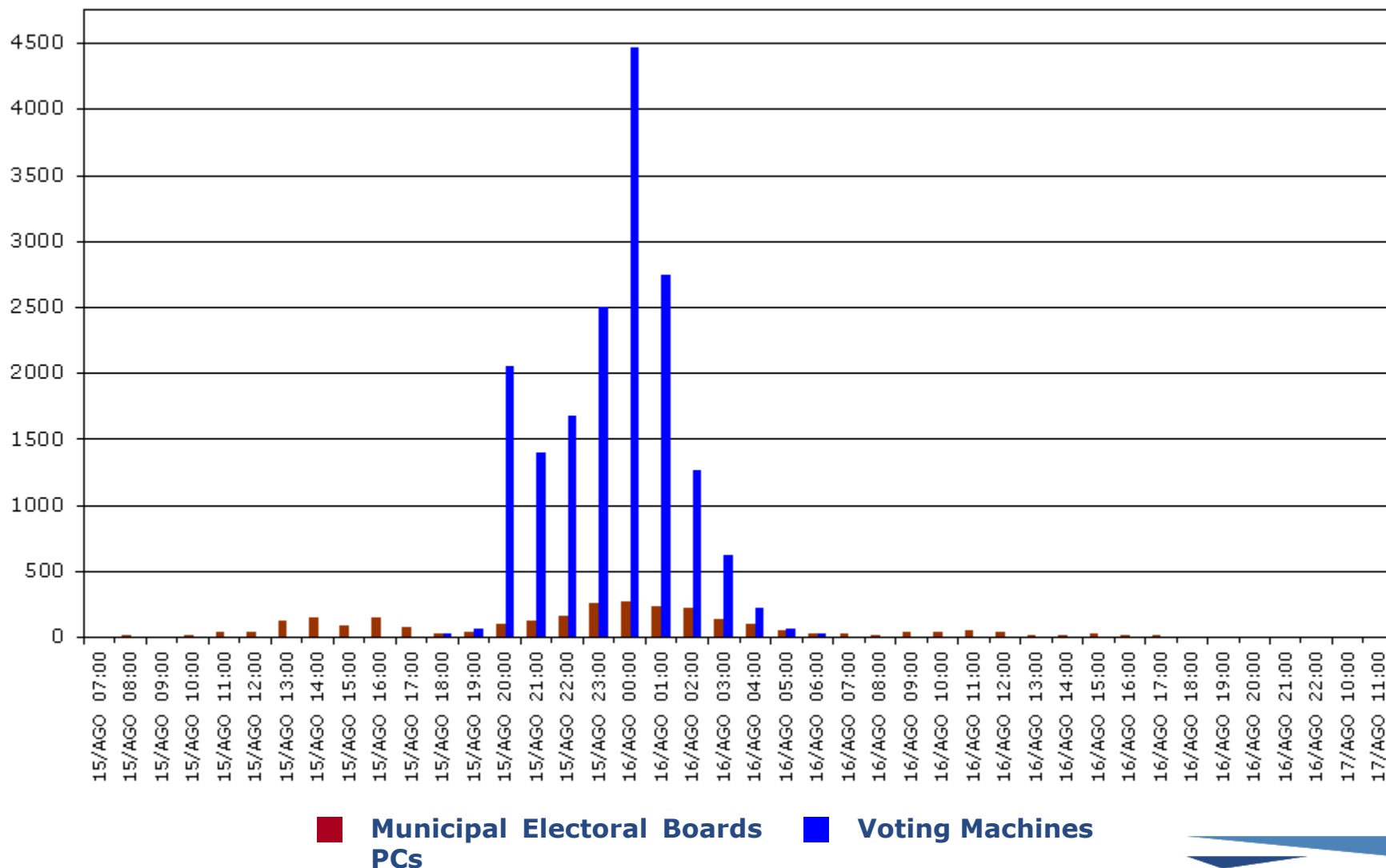
The investigation has been centered in the registries of sessions established by the voting machines and the electoral results. The following **anomalies** are detected:

- **Non observation of transmission schedules . Detected traffic before the closing time of the event.**
- **Heterogeneity of the data traffic in network as far as volumes of data , amount of packets and type of termination of sessions.**
- **Strong correlation between technological and electoral variables.**

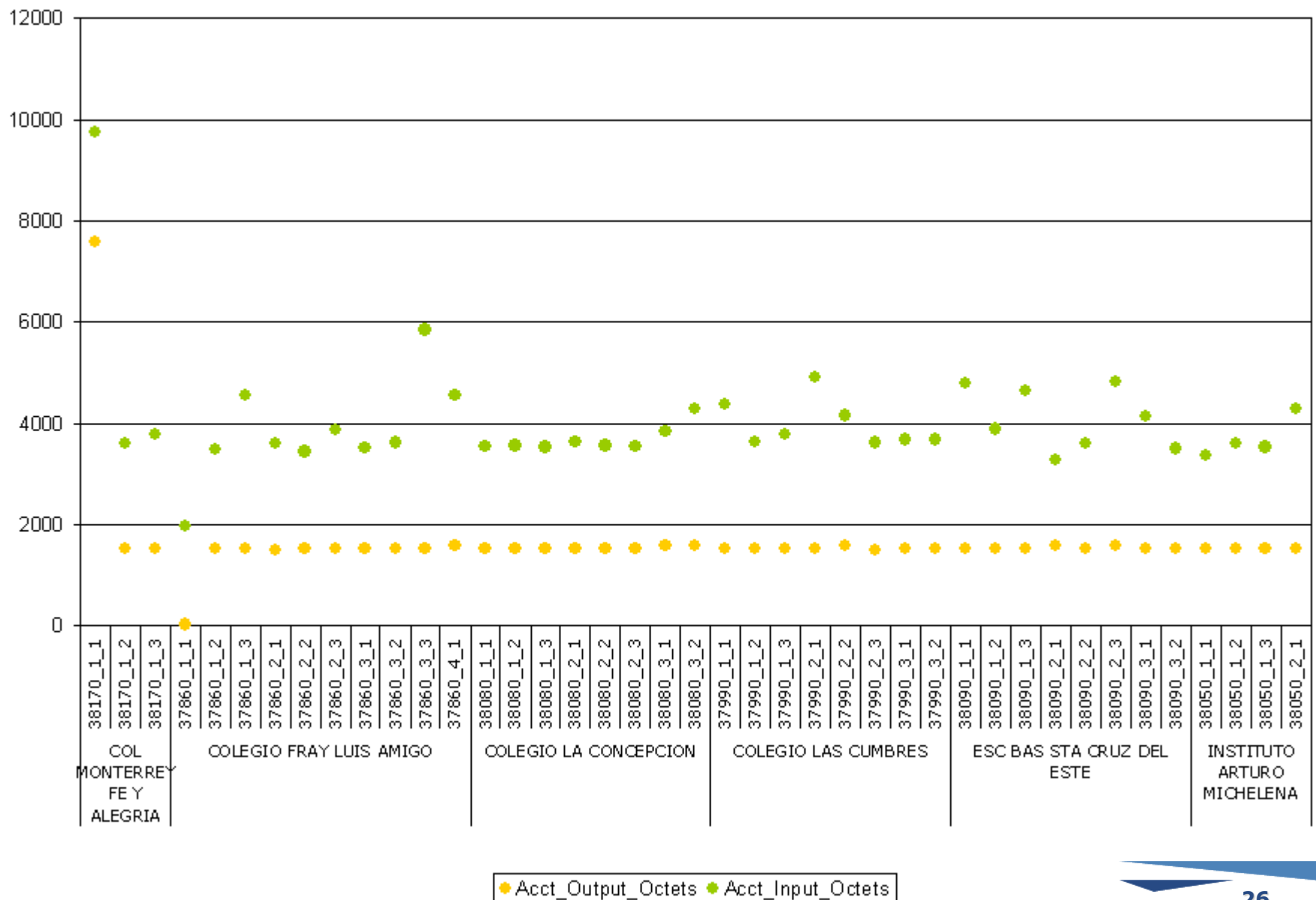
Findings - Transmission schedules



Established sessions in Wire Telephone Network



How to interpret the graphs that follow



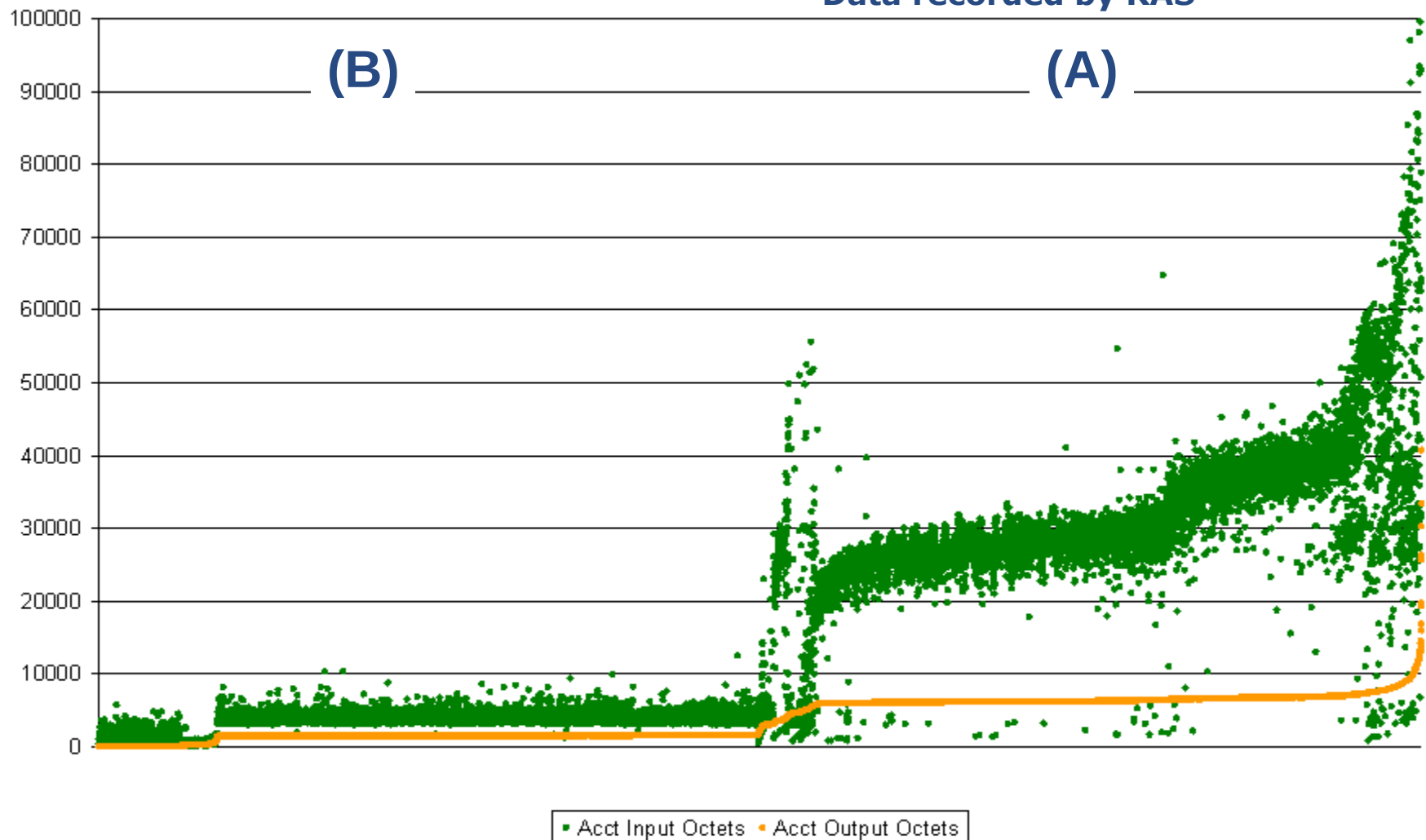
Findings - Heterogeneity



Bytes transmitted

Wire telephone network voting machines.

Data recorded by RAS

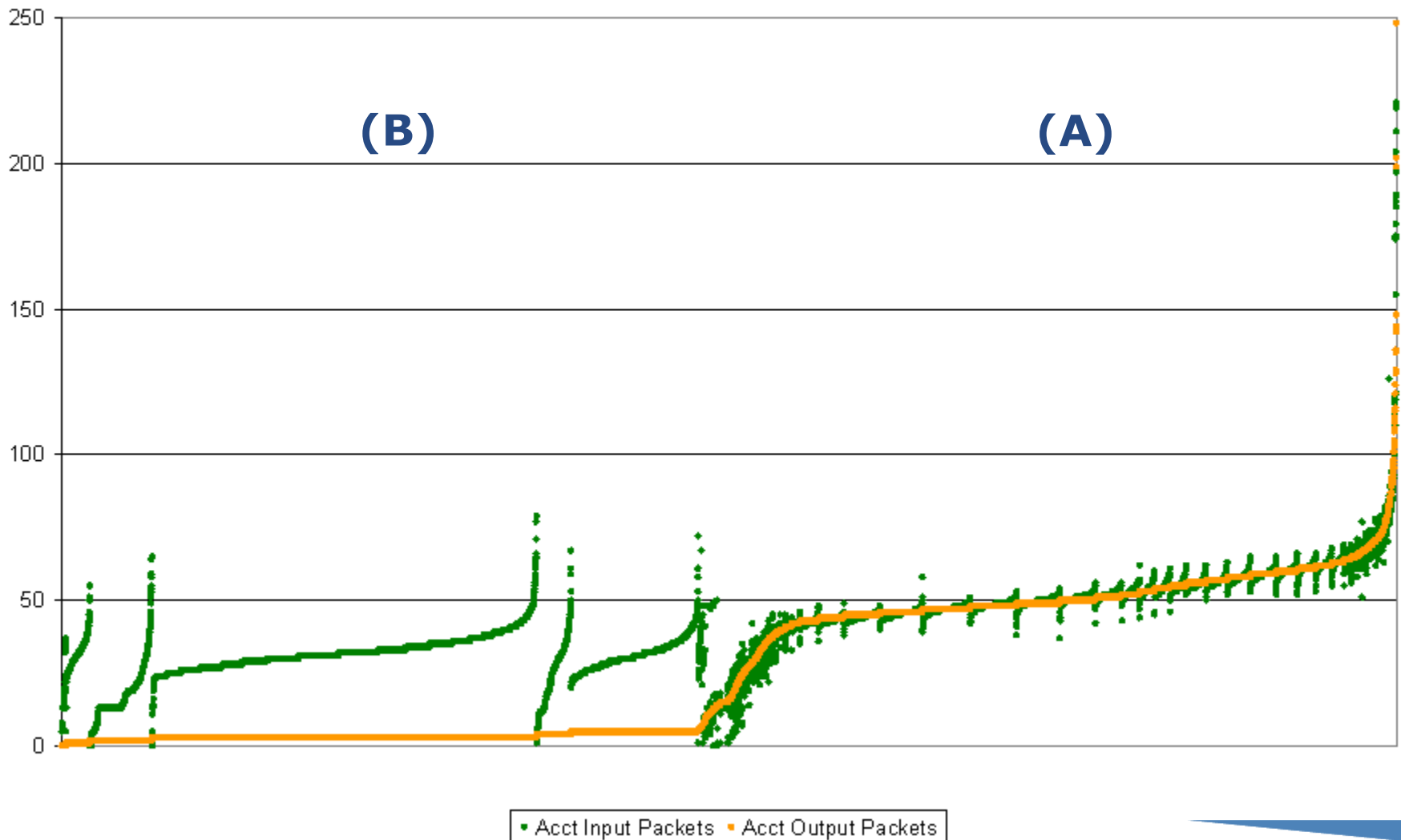


Findings - Heterogeneity - (cont.)



Number of packets

Wire telephone network voting machines. Data recorded by RAS

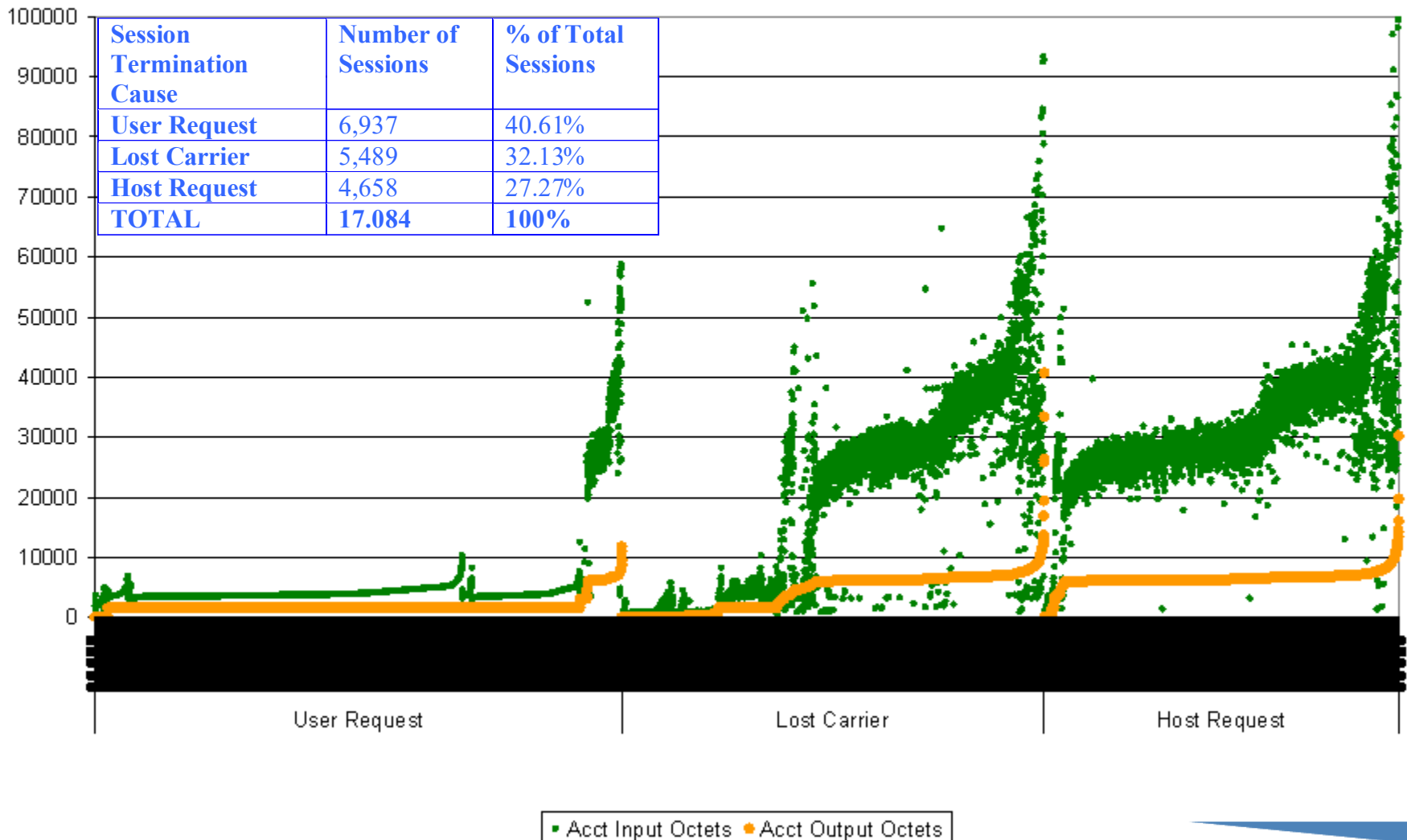


Findings - Heterogeneity - (cont.)



Bytes transmitted by termination of sessions

Wire network voting machines.
Data recorded by RAS

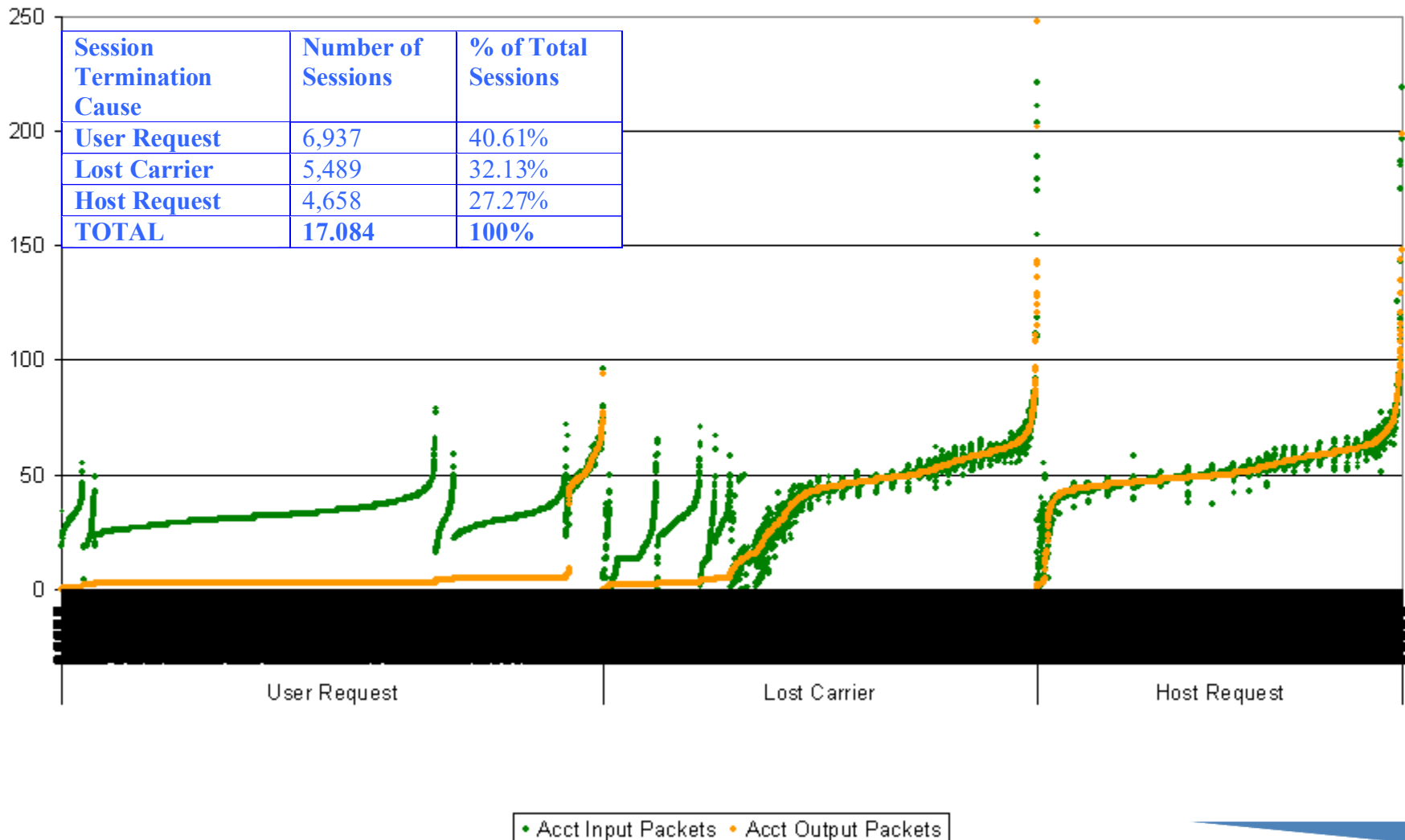


Findings - Heterogeneity - (cont.)



Number of packets by termination of sessions

Wire network voting machines.
Data recorded by RAS



Machines Classification according to Heterogeneity

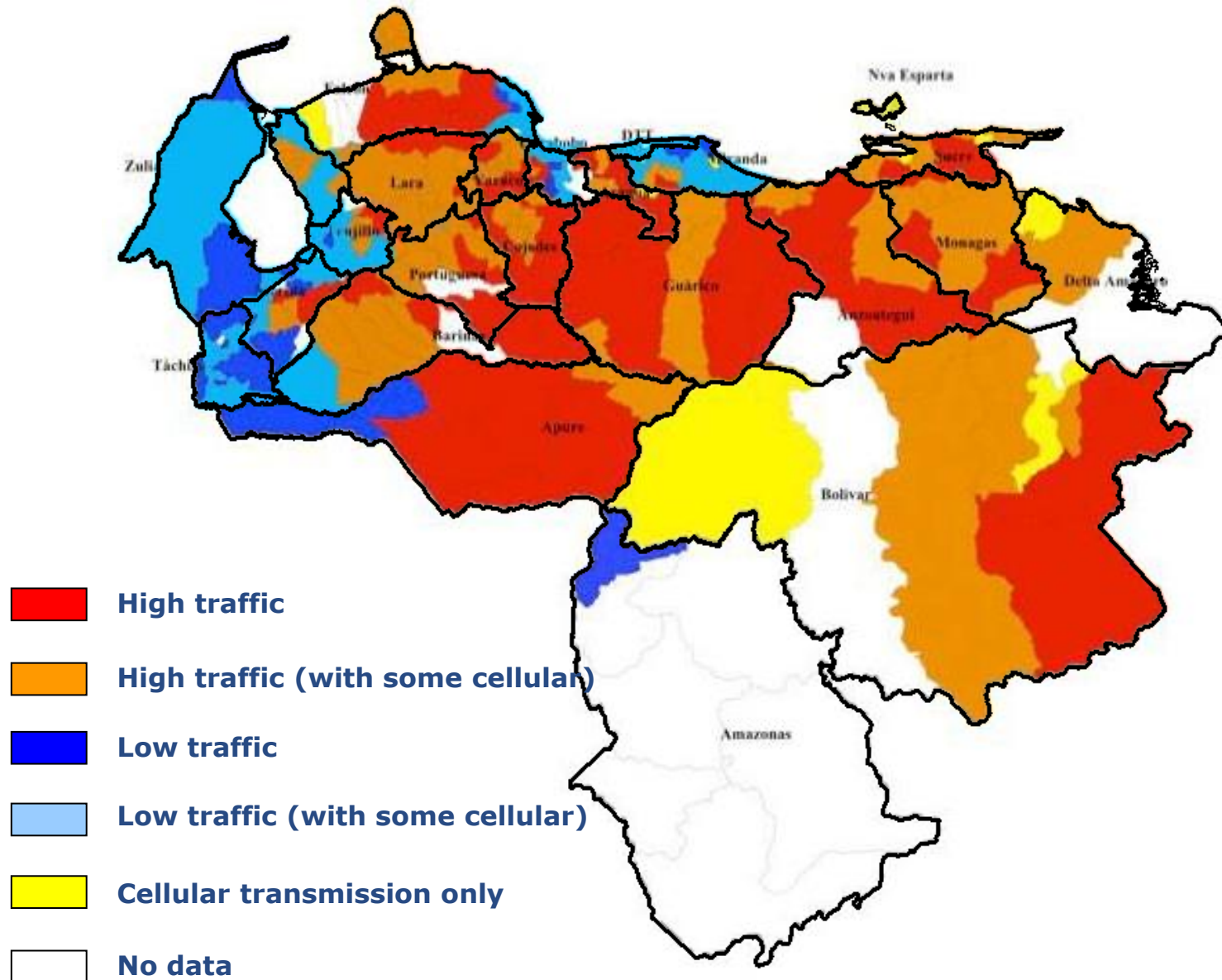


	High Traffic(A)	Low Traffic (B)	Cellular (C)	Total number of studied cases.
Voting Centers	1.876	1.573	972	4.421
Voting Machines in Voting Centers	* 8.185	* 7.383	** 3.124	18.692 (98,05% of automated PRR 2004)
Number of voting machines in each class	7.535	6.702	4.455	18.692 (98,05% of automated PRR 2004)
Total number of votes in each class and percentage of universe	3.695.415 43,44%	3.300.896 38,80%	1.357.733 15,96%	8.354.044 (98,20% of automated PRR 2004)

*: it includes voting machines with cellular transmission

** : it includes 0,5% of High Traffic voting machines

Traffic Distribution by Municipal Regions



Example of Data Transmission Pattern



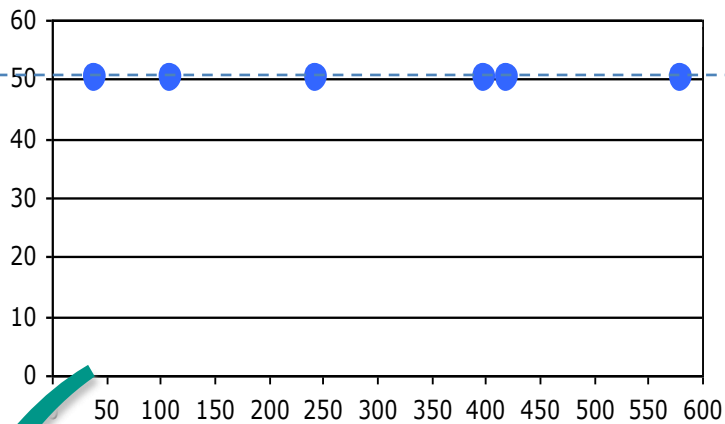
**Vote Totals
transmission**



**Individual
Vote
Transmission**

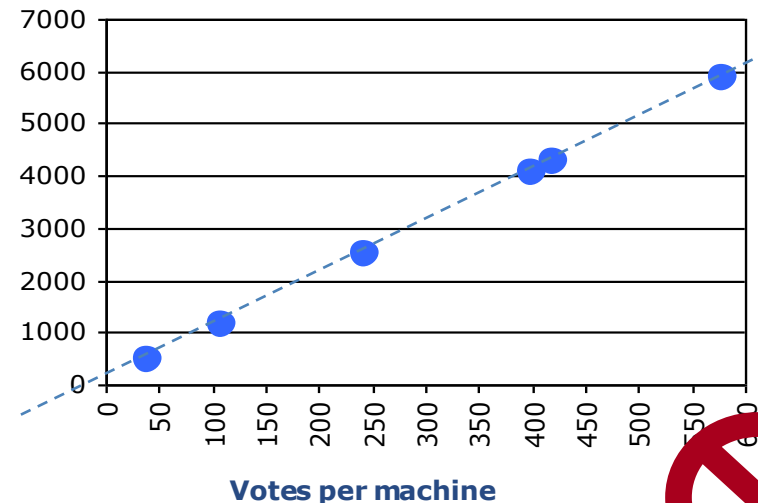


Bytes (data transmitted)



Votes per machine

Bytes (data transmitted)

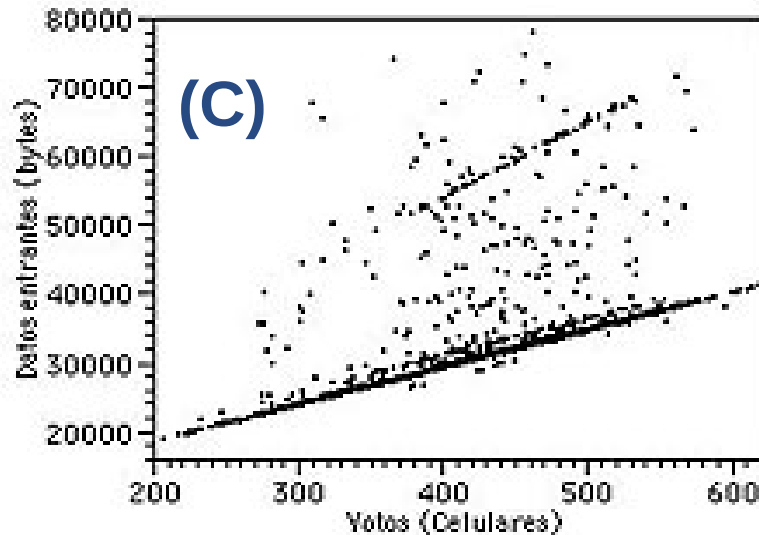
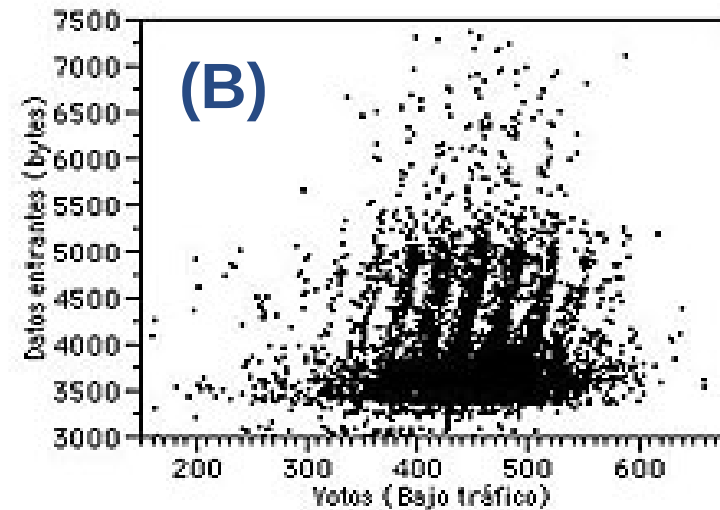
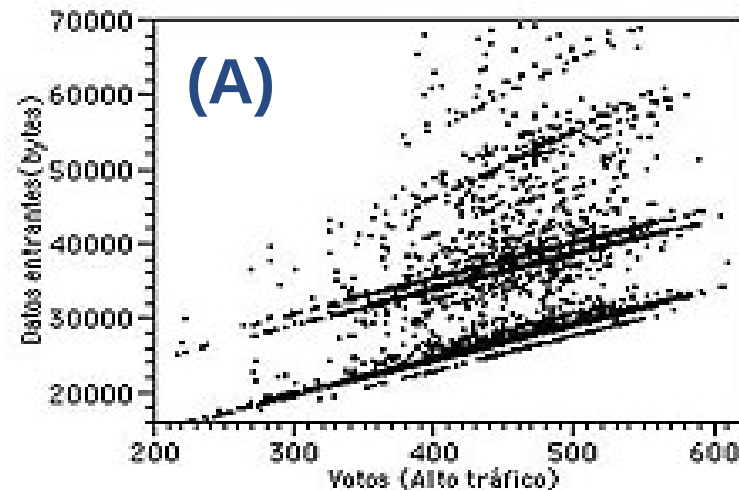


Votes per machine

● Represents a voting machine

● Represents a voting machine

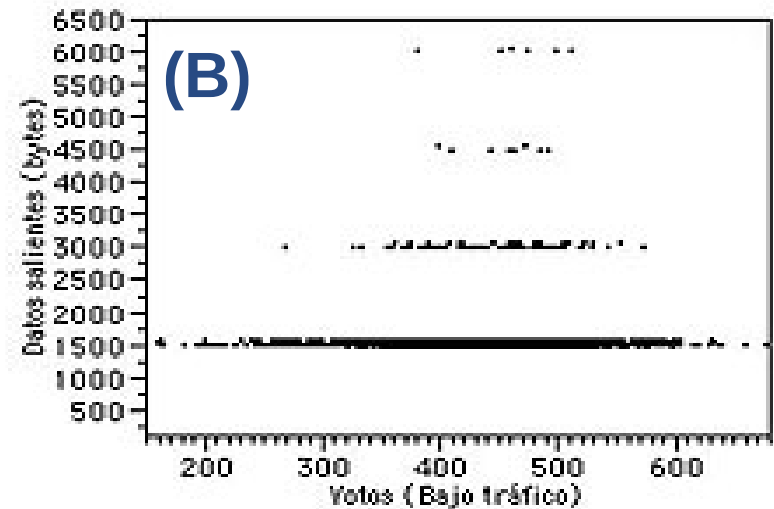
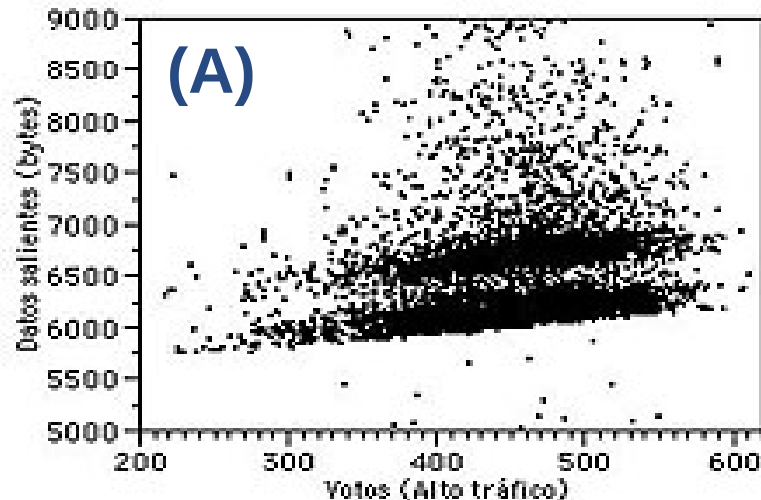
Data bytes transmitted vs. Electoral variables



Incoming data bytes versus Votes

for machines in groups: (A) High traffic (B) Low traffic (C) Cellular

Data bytes transmitted vs. Electoral variables



(C)

Para ver esta película, debe disponer de QuickTime™ y de un descompresor TIFF (sin comprimir).



Outgoing data bytes versus Votes

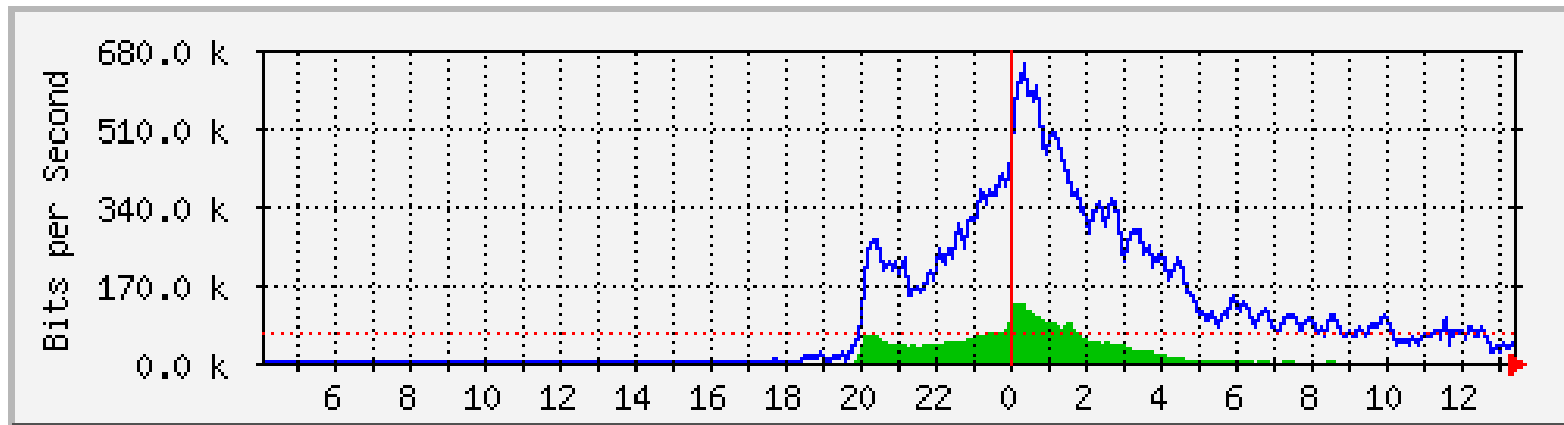
for machines in groups: (A) High traffic (B) Low traffic (C) Cellular

What is this graph telling us?



The statistics were last updated **Monday, 16 August 2004 at 13:28**,
at which time **'R-CNEL.cne2004.gov.ve'** had been up for **39 days, 21:54:35**.

'Daily' Graph (5 Minute Average)



Max **In**: 135.3 kb/s (211.4%) Average **In**: 16.8 kb/s (26.3%) Current **In**: 2088.0 b/s (3.3%)
Max **Out**: 647.3 kb/s (1011.4%) Average **Out**: 104.5 kb/s (163.4%) Current **Out**: 27.7 kb/s (43.3%)

Cantv report

Against any expectations, this graph shows that the outgoing traffic from the central servers towards the voting machines is much greater than the traffic received from these last ones!



V. Conclusions and recommendations

CONCLUSIONS



- **Unusual traffic in the data network previous to the closing time of the event.**
- **Bidirectional transmission of data in high unexpected volumes.**
- **The detection of heterogeneous patterns of data transmission in so far as: number of incoming and outgoing bytes and packets of information to and from machines; ways of termination of successful sessions, leads to infer that either executed programs in voting machines had more than one version or totalizing servers were discretionally administered.**



- A strong correlation between technological and electoral variables is found. The number of incoming and outgoing bytes are proportional to the number of total votes by machine rejecting the tally report transmission in the Cellular and High Traffic groups.

70% of voting machines do not show expected performances.

General Recommendations



- Clear up the electoral registry RE.
- Members of electoral tables should obtain a validation of credentials well in advance to the electoral event.
- The lists of electors and norms must be published in posters to the entrance of each voting center 30 days prior to the event at least.
- Impartial representation of political parties and independent observers should be present in all instances of the electoral process. Specially at the totalizing level as well as during transfer and storage of the electoral material.
- Participation of Plan Republic (Armed Forces) must be limited to safekeeping of voting centers and preservation of public order. Military personnel should not act as electoral agents.



- **All the equipment and operating systems should be certified by recognized and independent authorities.**
- **The source codes of voting machines and the software used by the central totalizing servers must be public.**
- **A complete and impartial audit of all components of the electoral system (software and hardware) before and after the event must be carried out.**
- **The use of electronic and blank electoral notebooks must be prevented to prohibit the 'floating voters' figure.**
- **The use of fingerprint catching machines must be suspended; in order to prevent any wireless connection between them and the voting-scrutiny-totalizing systems**



- **The automated tally reports must be printed and validated publicly through manual scrutiny of all the original ballot papers (machine receipts) deposited in the ballot boxes.*****
- **Only when the report is validated its transmission should be authorized.**
- **The invalid automated reports would be annulled and be replaced by a manual report to be sent to the corresponding regional or national electoral board.**



- **The manual electoral notebooks should be public documents which can be reviewed at the request of anyone.**
- **Logs of data transmission should be public documents to demonstrate the behavior of the traffic of data and to guarantee that only the official voting centers should be connected with the totalizing servers at the CNE.**
- **Logs of events in totalizing servers should be public documents to guarantee optimal performance of electoral administrative software**