The Electronic Vote in Venezuela

Technical evaluation of an electoral process

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

Agenda

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

Aims

- 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

Electoral System Outline

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

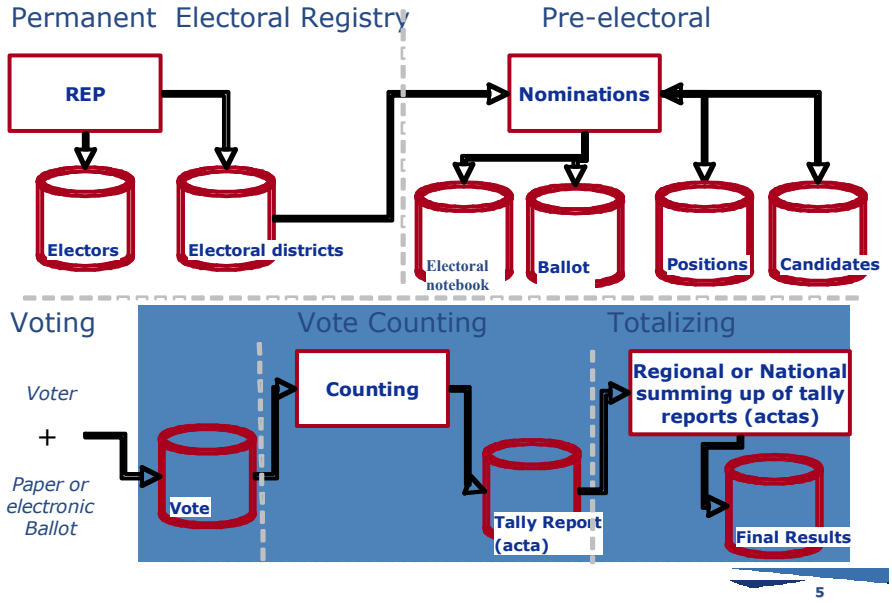
• **Permanent electoral registry (REP):** basic information on the electors and electoral districts.

• **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.

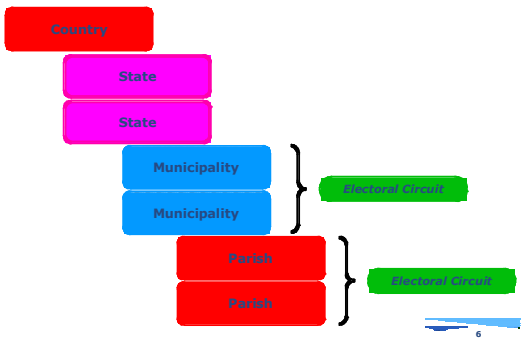
88,7% of PRR 2004 votes were cast electronically through touch screen machines, amounting to 8.6 MM votes out of a total of 9,85 MM

Electoral System Outline - (cont.)



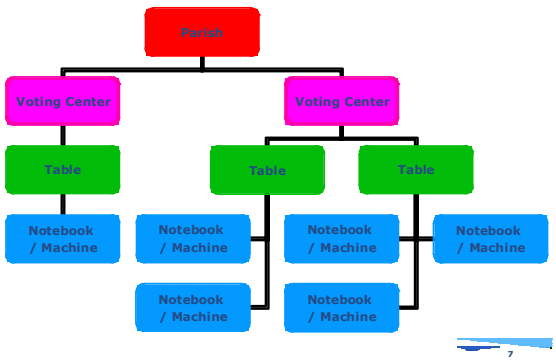
5

Venezuelan Political Organization

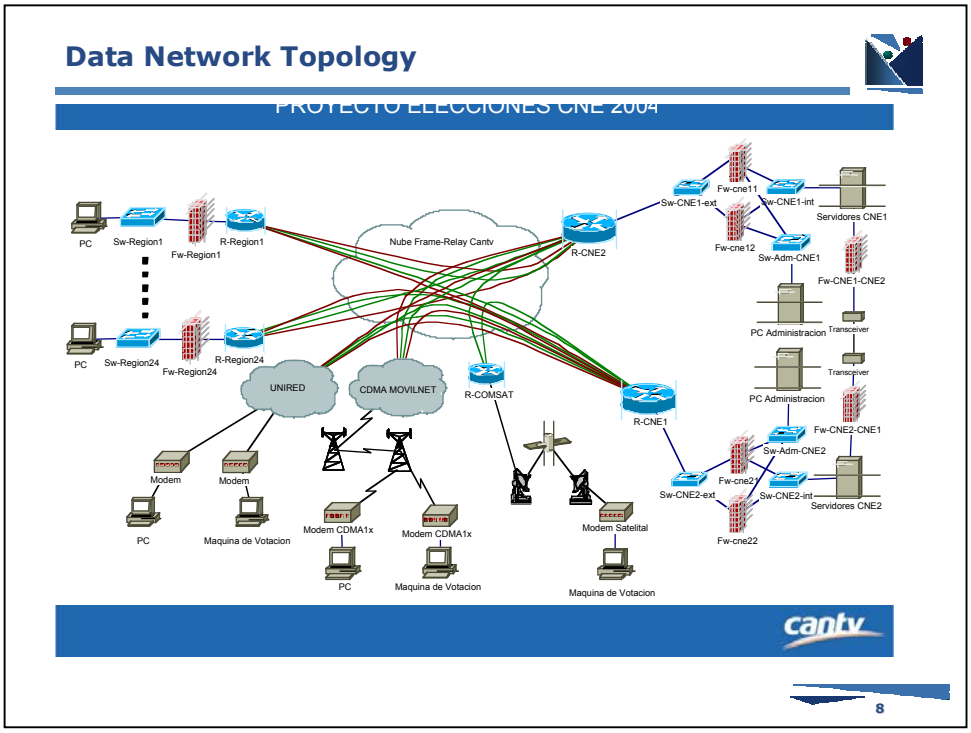


6

Electoral Organization



7



This graph is taken from the report of CANTV - CNE closure of contract. It shows the arrangement of voting machines and PC's of the Municipal Electoral Boards in relation to the main CNE totalizing servers and their back up in a parallel CNE-2. Voting machines and Boards PC’s were connected to totalizing servers either by wire telephone network (UniRed), cellular telephone network or by a satellite network.

CNE Electoral Conditions- Voting machines

• **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.

CNE Electoral Conditions- Voting machines

• **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.

In order to explain the point of the tally reports transmission, hypothetical examples of storage of data in memory and transmission of such for machines located in six different voting centers will be considered in next laminae.

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 06:02:00AM	16/08/2004 10:15:30pM	450	400	195	200	5
77788	4	3	15/08/2004 07:20:00AM	16/08/2004 06:32:03PM	500	420	250	240	30
55	1	1	15/08/2004 06:00:20AM	15/08/2004 11:55:09PM	600	580	320	160	0

11

In the above slide a hypothetical example for electoral results belonging to six different voting centers is shown. Several electoral variables for each center are described in the first top row.

Example - Individual Votes Memory Storing

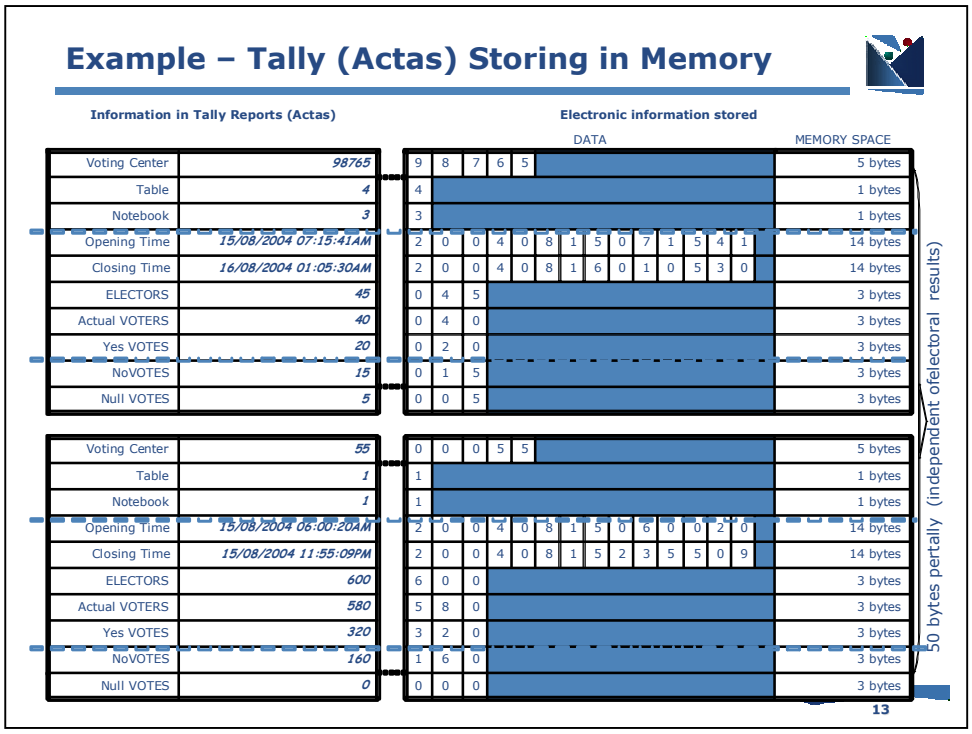
Vote Value	Vote Serial Number.	Vote	Serial Number	Amount of Bytes
NO	123000451	N	1 2 3 0 0 0 4 5 1	10 bytes
YES	123000452	Y	1 2 3 0 0 0 4 5 2	10 bytes
YES	123000453	Y	1 2 3 0 0 0 4 5 3	10 bytes
YES	123000454	Y	1 2 3 0 0 0 4 5 4	10 bytes
NO	123000455	N	1 2 3 0 0 0 4 5 5	10 bytes
NO	123000456	N	1 2 3 0 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 encripted way. Theoretically, once serial numbers and 'yes ' or 'no ' votes are encripted, 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.

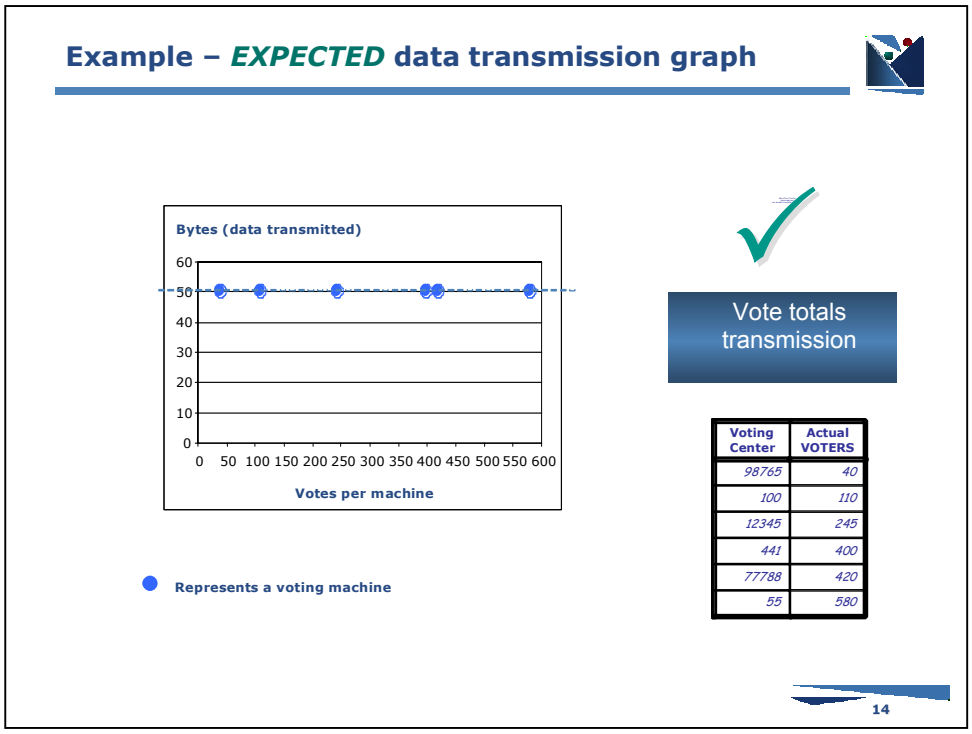
12

Above an example of how it is possible to store in the memory of the machine a sequence of votes with its respective identifiers serials is shown. The example indicates the possible amount of memory (in bytes) consumed by each vote. A byte is the information unit that occupies any symbol, that is to say, a number, a letter, a score sign or a blank space.



This is a hypothetical example of memory storing data contained in a tally report produced by a voting machine. The tally report includes voting center, table and notebook code numbers, number of assigned electors to the machine, number of actual voters that voted in that electoral event, number of total ‘yes’ votes counted by the machine, ‘no’ votes and null votes. In this example, the number of bytes saved in memory for the information in a tally is calculated. Note that the number of bytes does NOT depend on any electoral variable. The blue dashed horizontal lines represent the possible manner a message may be divided into packets of information to be transmitted: the first three rows may be in a packet, then the following five rows in a second packet and finally the last two rows in a third packet. Packets may have different payloads of information in terms of bytes.

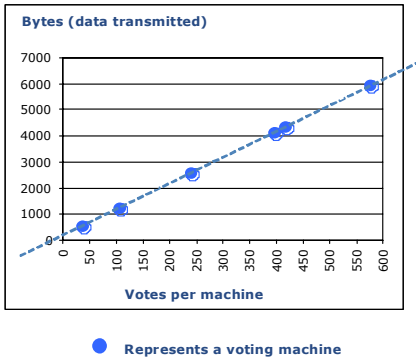
If the information in tally reports (actas) is the transmitted data to the remote central totalizing servers, the amount of transmitted bytes must be similar for every machine and must be independent of any electoral variable. In this example the number of total votes (equivalent to number of actual voters in each machine) was used as electoral variable. The various blue points in the graph represent different machines transmitting data contained in their respective tally reports. They transmit the same volume of data in bytes despite different numbers of votes were registered.



As before different blue points in the graph below represent different machines individually transmitting stored votes in memory, the number of bytes transmitted by each machine is a multiple of the number of bytes that corresponds to a single vote. This behavior in the transmission is not justified because the counting of votes must be made by the local machine. It does not have to send votes anywhere else to be added remotely with a program different from the one in the voting machine.

Example – NOT *EXPECTED* data transmission graph

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



15

CNE Electoral Conditions- Voting machines

• 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.

16

CNE Electoral Conditions- Totalizing servers

• **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.

Two sets of totalizing servers (near 200 each) located in two different CNE centers were used: one in the premises of the Consejo Nacional Electoral (CNE) and another one, apparently, in the Ministry of Science and Technology. This last one was a contingency center that would operate only in case of failure of the main totalizing center.

CNE Electoral Conditions- Results transmission

• **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.

Expected behaviour of electoral process

• 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.**

Expected behavior of electoral process

• 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

Sources of information for analysis

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

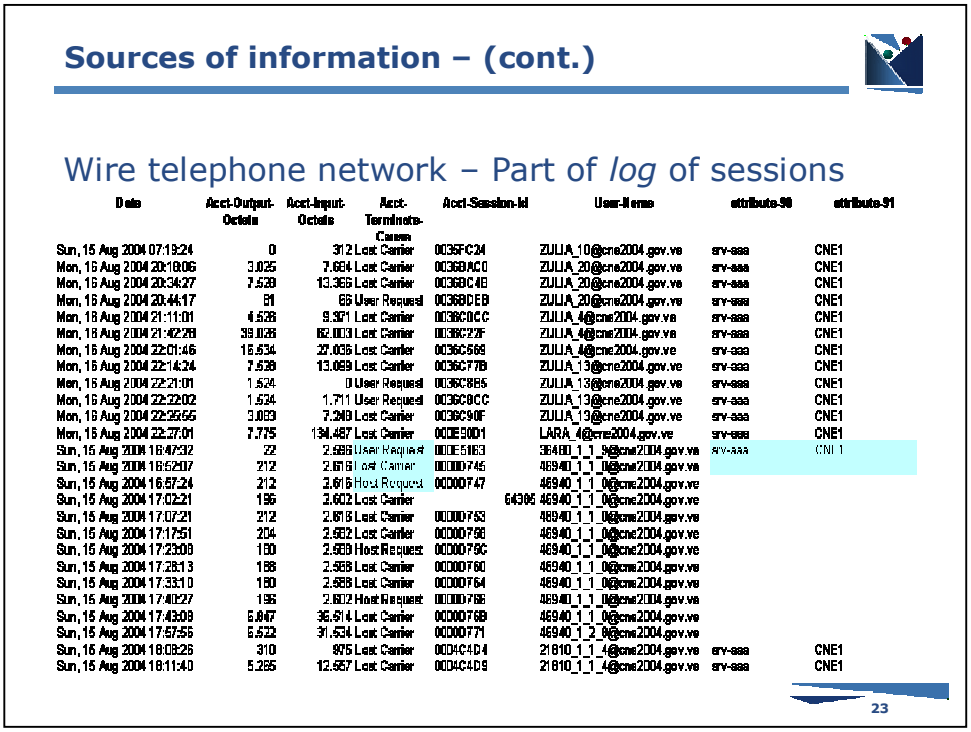
- Log of sessions established between voting machines and the CNE totalizing servers through the wire telephone network of CANTV.
- Log of sessions between the voting machines and the totalizing servers of the CNE through the cellular telephone network of Movilnet (CANTV subsidiary).
- Official results 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.

The slide below shows a sample page extracted from the log of sessions established between voting machines in the wire network and CNE tally servers. Few columns -but the most relevant ones- are shown. The first column shows date and time of the established session, the second and third one the amount of bytes (an octet is equivalent to a byte) transmitted to machines from totalizing servers and from machines to servers respectively. The forth column indicates the cause of termination of sessions: if terminated by the voting machine then it is a case of 'user request', if the totalizing server ends it a 'host request' is reported . "Lost carrier' denotes a lost session either by a network failure or errors in connections.

The 'user name' column indicates which machine was connected to the CNE totalizing server. In case the code starts with a State name followed by a digit tells us that the machine was a municipal electoral Board PC, with that digit as code number. In case of a number with various digits separated by underscores shows that the machine corresponds to a voting center with the first digits as code number, the second digit number represents the table number and the rest the electoral notebook number and a control digit.

Attributes 90 and91 indicate which type of server authorized the access to the session and the server that was connected to the voting machine. This log of sessions use the default definitions of RADIUS variables most commonly employed by the telecommunications companies to record the service accounting.

It is worth noting that this log showed nearly half of blank rows in Attribute 90 and 91. This could happen either because the AAA servers for accounting used different versions of programs or they were deleted for some unknown reasons.



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	0036FC24	ZULIA_10@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 20:19:06	3.025	7.684	Lost Carrier	0036BAC0	ZULIA_20@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 20:34:27	7.539	13.366	Lost Carrier	0036BC4B	ZULIA_20@cne2004.gov.ve	srv-aaa	CNE1
Mon, 16 Aug 2004 20:44:17	81	65	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 21:42:29	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	7.539	13.069	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	00DE90D1	LARA_4@cne2004.gov.ve	srv-aaa	CNE1
Sun, 15 Aug 2004 16:47:32	22	2.686	User Request	00DE5163	36480_1_1_9@cne2004.gov.ve	srv-aaa	CNE1
Sun, 15 Aug 2004 16:52:17	212	2.616	Lost Carrier	00000745	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 16:57:24	212	2.616	Host Request	00000747	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:02:21	196	2.602	Lost Carrier		64305 46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:07:21	212	2.616	Lost Carrier	00000753	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:17:51	204	2.602	Lost Carrier	00000758	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:23:08	180	2.568	Host Request	00000759	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:28:13	186	2.568	Lost Carrier	00000760	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:33:10	180	2.568	Lost Carrier	00000764	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:40:27	196	2.602	Host Request	00000766	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:43:09	5.847	36.514	Lost Carrier	00000769	46940_1_1_0@cne2004.gov.ve		
Sun, 15 Aug 2004 17:57:56	5.522	31.534	Lost Carrier	00000771	46940_1_2_0@cne2004.gov.ve		
Sun, 15 Aug 2004 18:08:26	310	975	Lost Carrier	00D4C4D4	21810_1_1_4@cne2004.gov.ve	srv-aaa	CNE1
Sun, 15 Aug 2004 18:11:40	5.295	12.957	Lost Carrier	00D4C4D9	21810_1_1_4@cne2004.gov.ve	srv-aaa	CNE1

Findings

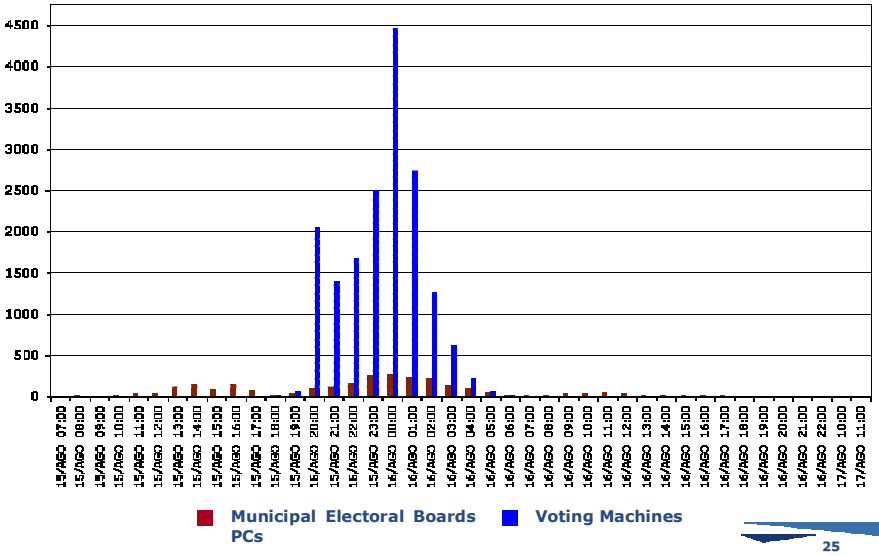
The investigation has been centered in the registries of sessions established by the voting machines and the electoral results. The following **anomalies** are detected:

- **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.**

24

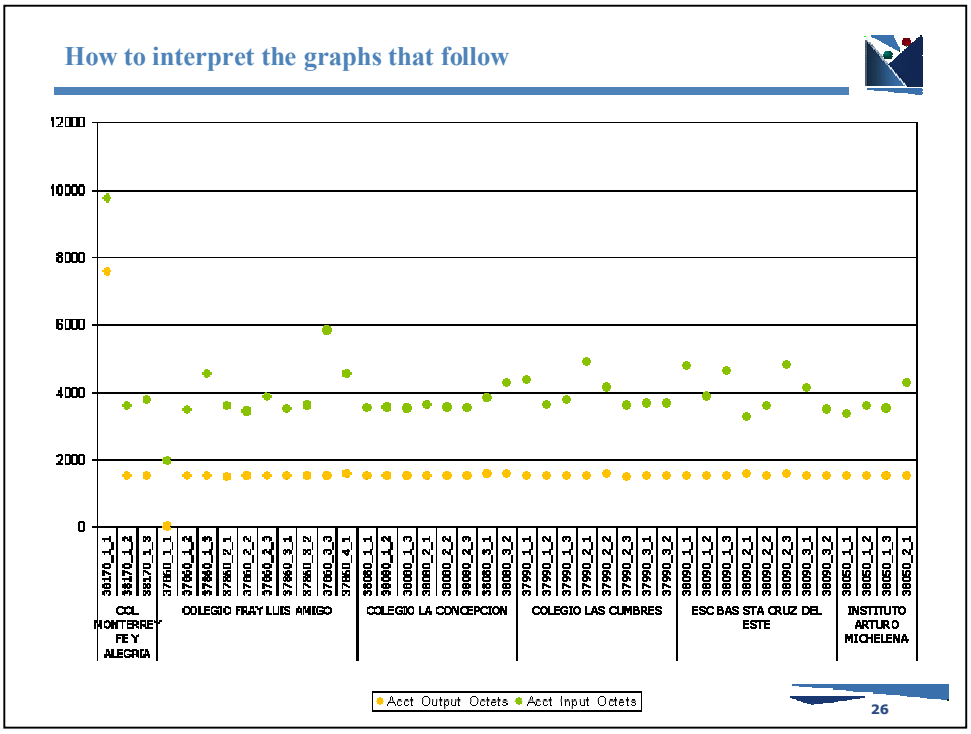
Findings - Transmission schedules

Established sessions in Wire Telephone Network



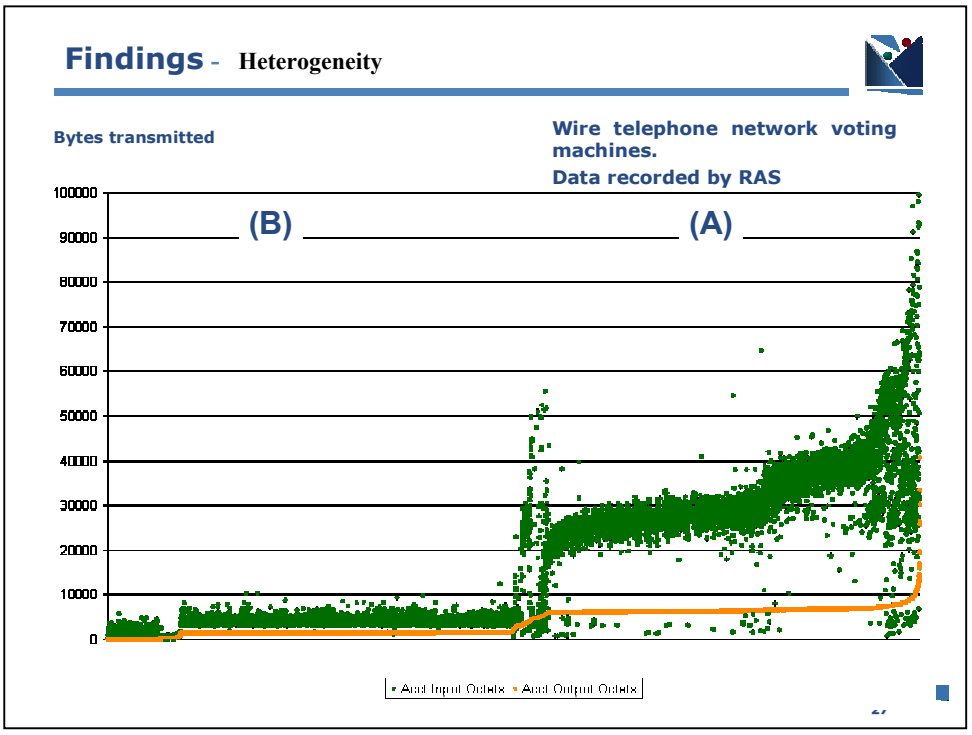
25

In this graph the number of sessions established between machines and totalizing servers are shown by time intervals. The amount of votes received by the CNE between 20:00 hours and 00:00 was around a million votes. The Municipal Electoral Boards began to transmit from the 07:30 hours and the voting machines from the 16:30 hours.

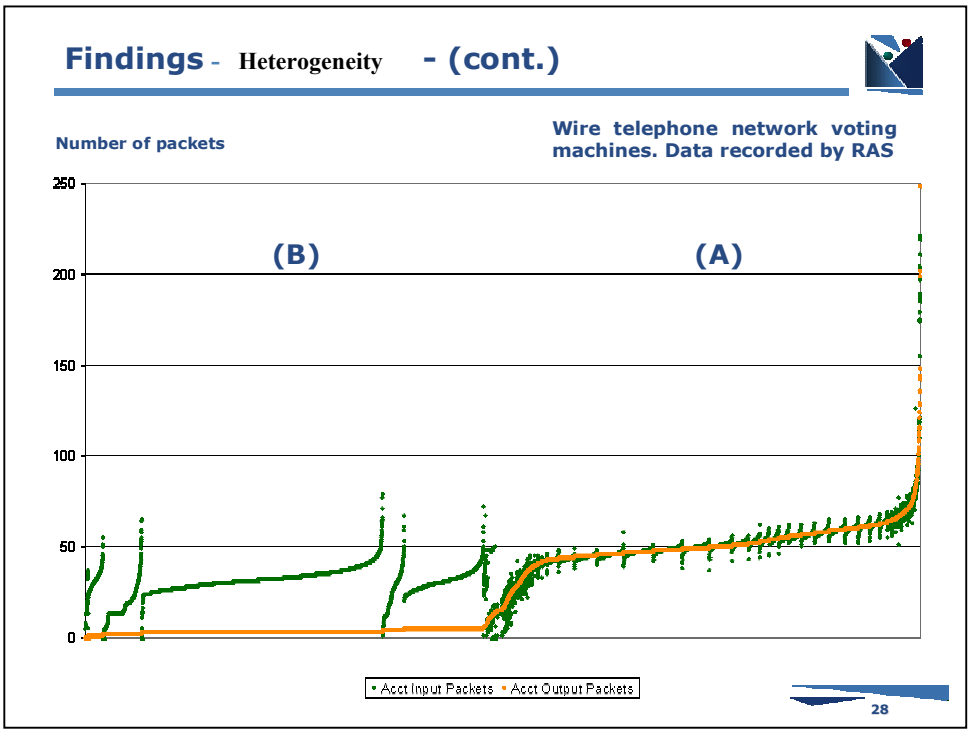


This graph contains actual data produced during the PRR (around 40 machines). Voting machines (its code numbers) from several voting centers are placed on the horizontal axis and the number of bytes transmitted to and from the voting machines are plotted. In the vertical axis the number of transmitted bytes are indicated . To every voting machine there corresponds two coloured points , one of them represents bytes used to transmit data to totalizing servers and the other one bytes received from servers.

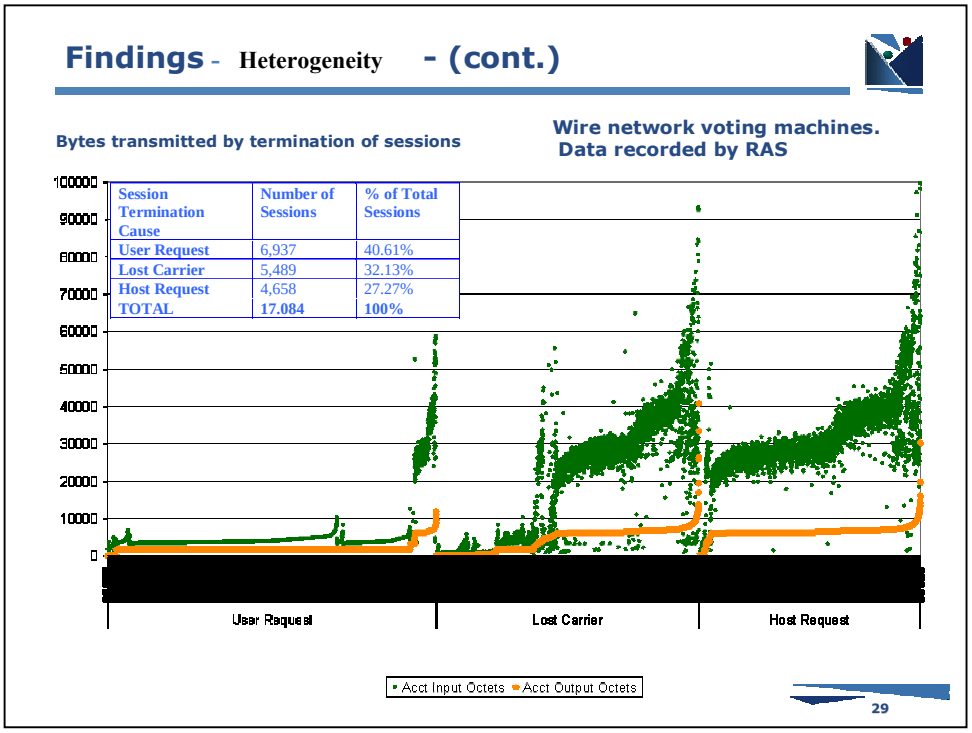
In the graph shown in this page as in the previous slide, the volume of bytes transmitted and received by all voting machines in the wire telephone network (tens of thousands of points) are represented. The heterogeneity of the behavior is indicated. It shows that programs were executed in different ways in the machines. This behavior gave way to a classification of machines in two groups, group (A) for machines that reported high volumes of data transmission (to the right of graph) and the group (B) with lower transmission volume compared to (A).



The heterogeneity also is observed in the transmission of information in packets. A message of a determined number of bytes can be divided in several packets for its transmission, the program executed to divide the information was different in two groups of machines. Again the heterogeneity corresponds with groups (A) and (B), being the group(A) the one that reports the same number of packets in both directions (to the right of the next graph).



Below volume of data bytes according to the termination cause of sessions are plotted. Heterogeneity in behavior is shown indicating that different programs were executed in data transmission. Notice an extremely unexpected high percentage of 'lost carrier' cases.



Machines Classification according to Heterogeneity

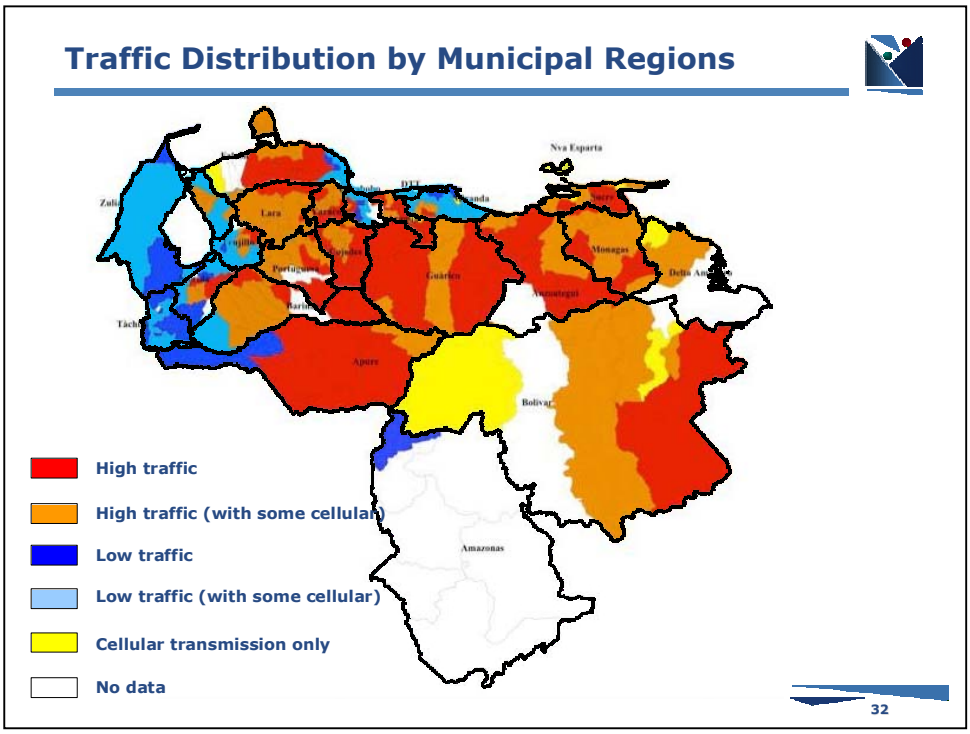
	High Traffic(A)	Low Traffic (B)	Cellular (C)	Total number of studied cases.
Voting Centers	1.876	1.573	972	4.421
Voting Machines in Voting Centers	* 8.185	* 7.383	** 3.124	18.692 (98,05% of automated PRR 2004)
Number of voting machines in each class	7.535	6.702	4.455	18.692 (98,05% of automated PRR 2004)
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

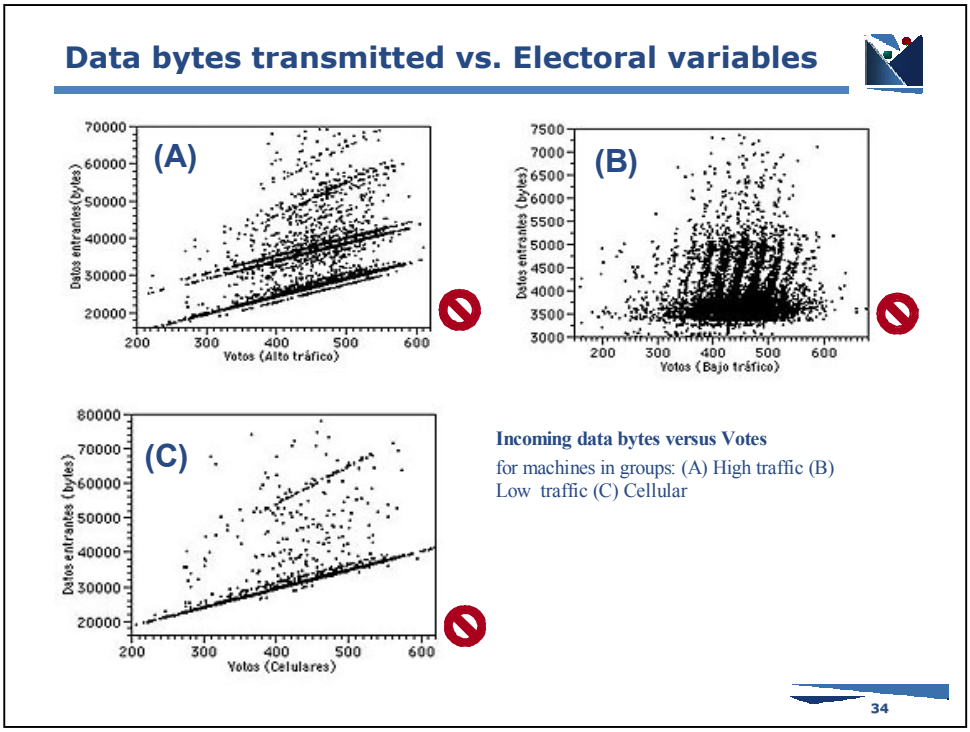
31

In this table, cellular transmissions are included. High and Low traffic refers to wire telephony only. Notice the high percentage of cellular transmissions. Nevertheless, these machines were not considered for the 'universe' audited in either of the programmed audits (neither the one ran the same day of the event nor the one performed by the Carter Center and CNE).

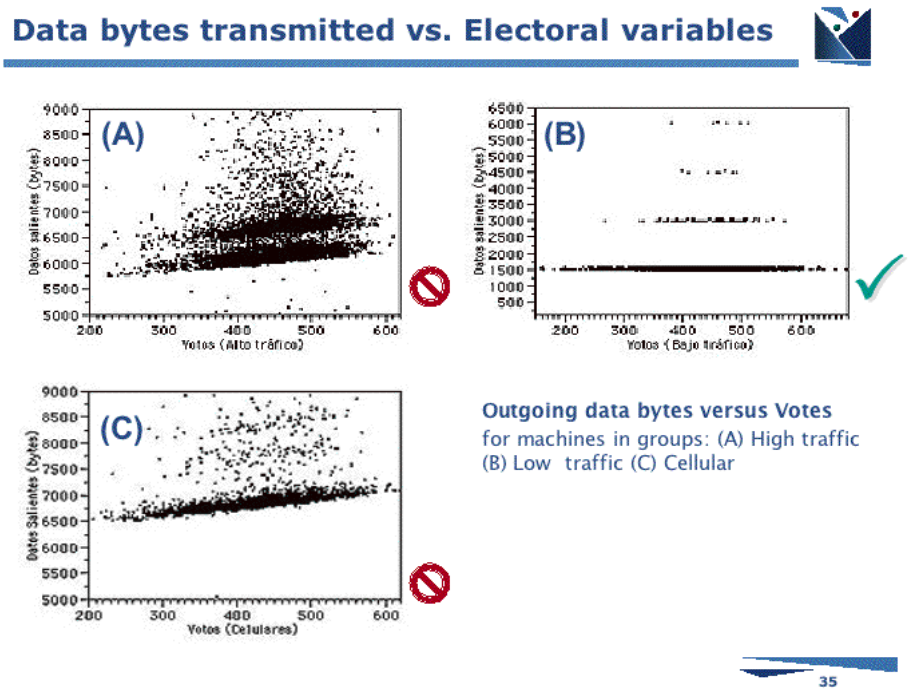


This Venezuela map, divided by municipial regions, shows the localization of voting centers with different types of data transmission . Only one municipality in the Carabobo state shows a mixture of voting centers transmitting data in High Traffic and Low Traffic classes but they are registered in different parishes. The rest of 'municipios' (around 300 of them) show a homogeneous behavior with respect to the type of traffic. It should be noted that there is no correspondence between the geographic areas attended by different regional telecommunication central units and the electoral districts. It means that the traffic distribution obeyed electoral reasons.

In what follows, data transmitted from and to voting machines compared to the number of votes reported is shown. Compare the patterns shown with the above discussion about expected behavior in transmissions fron the point of view of the electoral normative.

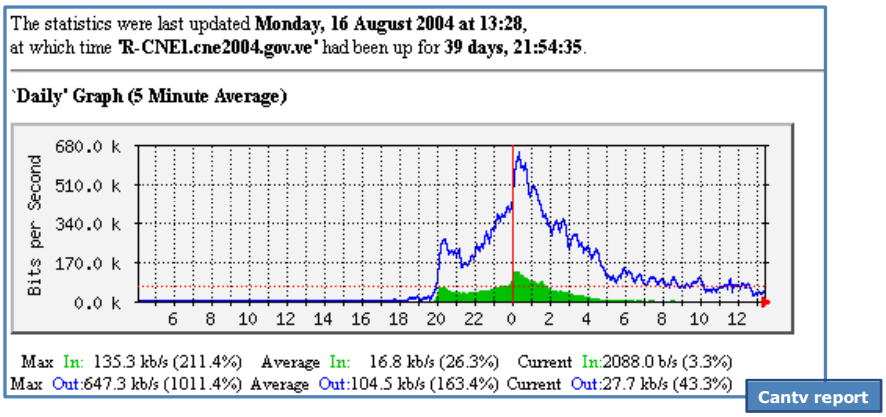


In these graphs, the amount of bytes in the incoming data transmission, according to log of sessions of wire and cellular telephone transmissions, are plotted against electoral variables. In this case, the amount of votes reported in each machine according to official results of the CNE. Each point represents a voting machine, its projection onto the horizontal axis indicates the total number of votes that each particular machine reported and its projection on the vertical axis indicates the amount of bytes used in the transmission of results. The pattern of proportionality between the amount of bytes with the votes reported in the High Traffic (A) and Cellular (C) groups, and in a smaller degree in the Low traffic (B) group, indicates that vote totals were not transmitted only. The linear patterns with very defined slopes (47 bytes per vote) are related to high volumes of traffic as the vertical axis scales show. As the program executed by voting machines for vote storage and transmission is not known, it is not possible to assure that all or a partial number of individual votes were transmitted. It is relevant to notice that in High Traffic voting centers, one finds that one or two machines of the same table, out of three contiguous machines, could use up to 10,000 bytes more to transmit similar information. In the graph of the (A) group the straight longer and more visible parallel lines have the same slope, the machines in the top straight line transmitted 10,000 bytes more than the machines in the bottom straight line but both may belong to the same table of the same voting center.



Here the vertical axis indicates the amount of bytes received from the central servers *according to the log of sessions*. The pattern of proportionality between amount of bytes and reported votes in the High Traffic (A) and Cellular (C) groups indicates an anomalous behavior, highly because it is not expected that totalizing servers communicated information related with individual votes to the voting machines. The linear patterns with very defined slopes are related to high volumes of traffic as the vertical axis scales show in the High Traffic (A) and the Cellular (C) groups. Also in the High traffic (A) and the Cellular (C) groups the slopes of both clouds of points are aproximately the same ranging from a byte per vote in (A) to a byte and a half per vote in (C). The pattern of the Low traffic (B) group, in this case, does not show any relation with votes, the volume of bytes also is small compared with the other groups. **This latter pattern of behavior IS the expected one in all cases for all machines and in any direction of communication.**

What is this graph telling us?



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

This graph shows the bandwidth used by the network during the PRR event. It was taken in real time in the entry router to the internal CNE network, it is in all versions of the contract closure report of CANTV and CNE. According to the documents this graph was taken from the WAN region (from 'the entrance door ' to CNE) and shows a blue curve of outgoing traffic (Out) in units of kilobits per second which is much greater than the incoming traffic. This graph is produced by a MRTG application in the routers of data networks to monitor several variables associated with data transmission. The default configuration of this program uses the convention of blue curve for the outgoing traffic and the green one for the incoming one.

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.

CONCLUSIONS - (cont.)

- 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 for Electoral Results transparency

- **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.**

Pre-Electoral Technical Recommendations

- **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**

Electoral Technical Recommendations

- **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.**

Post-Electoral Technical Recommendations

- **The manual electoral notebooks must 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 are 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.**