Constraints of the integration of smart cards in a distributed medical record system

Contraintes d'intégration d'une carte à puce intelligente dans un système réparti de dossiers médicaux portables

Rachid O. Zaïane et André Gamache[1]
Département d'informatique, Université Laval
Sixièmes Journées Internationales des Sciences Informatiques,
Tunis 20-21-22 Mai 1992

Summary

The design of a Portable Medical Record (PMR) smart card based system introduces a new passive component in the system delivery of medical services to end users. This new carrier of medical data, the PMR, aimed at sharing health information, should also comply with every bit of medical ethics and of government regulations regarding confidentiality and access to medical information. The Québec PMR system is being designed in order to reinforce these constraints and to be independent from any major technological choice. This approach involves several technical challenges. The first is the impact of accumulating data in various controlled access zones while managing memory space to delay the unavoidable saturation state. We propose certain strategies for memory management and the use of compression technics. The proposed system has a three-level architecture: Application software, Interface and Driver. Each layer has its own specific functions and components; the information flows among them according to a predetermined communication protocol. The smart card based system to be tested will give us better clues on behavior of health professional and patients towards a new computerized tool that some may regard as an intruder in the health care professionnal-patient relationship.

Key words: Smart Card, Portable Medical Record, Data compression, Computerised medical system, Secure access to data.

Résumé

La carte à microprocesseur est un support informatique innovateur qui marque un nouveau stade dans l'informatisation et la décentralisation des données sensibles. Elle constitue un outil très intéressant et fiable pour la collecte et la diffusion rapide de l'information médicale ainsi que son partage sécurisé. L'intégration de la carte à puce intelligente dans un système de gestion des données de santé pose plusieurs problèmes tant sur le plan de la structure de données que celui de l'espace physique requis pour stocker un dossier médical. Le système de Dossier Médical Portable (DMP) que nous proposons tient compte de l'éthique médicale, de la réglementation concernant l'aspect confidentiel et l'accès aux données médicales et tend à relever les défis posés par la multiplicité des acteurs, la multiplicité des technologies qui adhèrent à différents standards et le problème de la saturation de la mémoire. Des expériences utilisant des cartes à mémoire soulignent l'importance des problèmes de saturation des cartes et de l'accès sécurisé aux données. Notre architecture à trois niveaux montre une structuration réfléchie du système d'information. Nous présentons des solutions à la saturation de la mémoire de la carte à travers la conception du dossier portable, des politiques de gestion de la mémoire et la compression des données médicales.

Mots-clés: Carte à puce intelligente, Carte à mémoire, Dossier médical portable, Compression des données, Système médical informatisé, Accès sécurisé aux données.

---

1. Auteurs' address: Département d'informatique, Faculté des Sciences et de Génie, Université Laval, Québec, Québec, Canada, G1K 7P4 fax: (418) 656-2324, e-mail: gamache@vm1.ulaval.ca

Outline:

Part 1:

- Design philosophy and constraints of PMR
- Implementation challenges
- Data structuring and mapping

Part 2:

- Memory management
- Simulation: some results on saturation

Part 3:

- Compression techniques and
- Preliminary results with medical records
- Conclusions

Part 1

Design Philosophy of the QPMR (Québec PMR) [Cantin 1991]

1. Health Care Professionals (HCP) as providers of medical services and representatives of their professional body should be directlyou indirectly involved in the design of the QPMR:

main user groups: medical doctors
pharmacists
nursing personnel (under supervision)

2. The proposed system for managing the QPMR, should be tested and monitored extensively within a controlled pilot project prior to its implementation on a large scale basis: population of 6 million;

3. Health Care Professionals, end users and external peers should participate in assessment of this pilot;

4. The pilot project should provide the necessary data to evaluate the feasibility of generalizing the system throughout Québec;

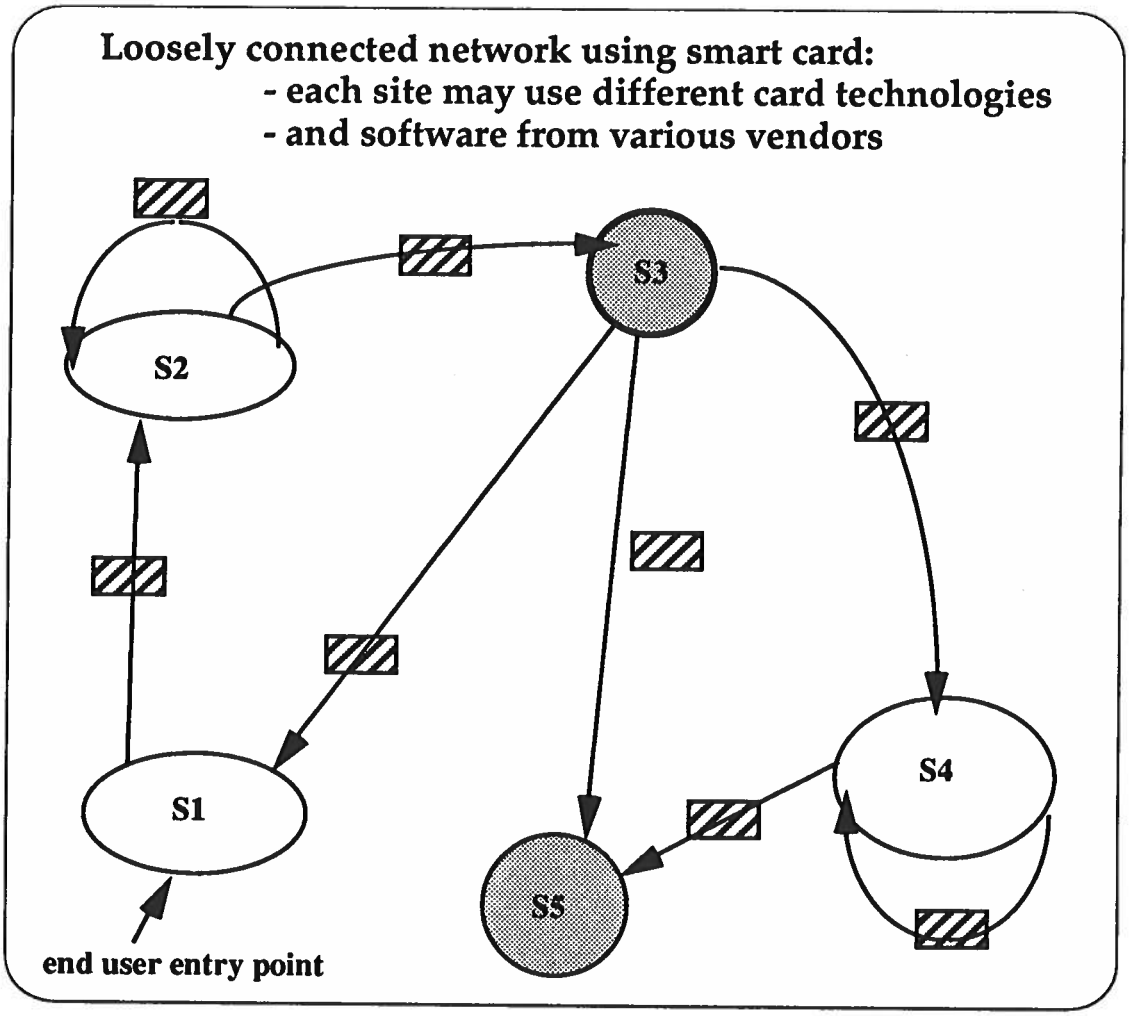
5. The software system should be highly reliable and able to cope with expected rapid technological obsolescence in this field of Integrated Circuit (IC) [gamache 1990];

6. Each HCP should be accountable for every bit of information stored on the QPMR: data are stamped (with signature and date) and persistent.

Main goal (from an information system perspective)

Improving the quality of medical and pharmaceutical services based on sharing reliable and update informations in a loosely connected network of care providers.

The information bearing media is the smart card; the point of services are mostly client-clustered and links are highly secured. On a long term basis, the node is expected to be heterogeneous in terms of hardware and software.



Québec Portable Medical Record (QPMR)

System's constraints [Cantin 1990]

1. The QPMR should reflect the needs of HCP as required by their decision making processes;

2. The QPMR should trace every transaction that both the patient and the HCP consent to write on;

3. The QPMR should be highly secured in order to guaranty the confidentiality of data;

4. No central repository of medical data should evolve from the use of QPMR; no "easy" algorithm could be used to reconstruct the population entire database (a very slow heuristic could exist);
5. The QPMR should convey information for authorized HCP on the basis of

predetermined access rights; under supervision, the data should be also accessible to the bearer;

6. Open system design: new application and new data elements may be added during the card life cycle without impairing previously defined operational applications;

Some design and implementation challenges

1. Modeling medical unstructured data:
   no universal minimal data set recognized;
   identification and relevance;
   content coding for consistency and space saving;
2. Full and strict implementation of all user access rights to medical data;

3. Highly effective User Application Interface designed and tested for each group of HCP;

4. Highly reliable system software: fault tolerance and transparency to technological changes is looked for with respect to smart card technologies;

Data structuring [Durant 1990]

Logical PMR (Application Level)

The QPMR is structured with logical zones; no reference to physical memory. Every application has a specific view of the logical PMR.

Logical zone

Every data to be entered by HCP belongs to a logical zone: a logical zone is a grouping of semantically related data elements without any reference to their access or protection rights;

---> we may have approximatively 45 logical zones in the QPMR
Logical transaction

All application view the PMR as a logical structure;

Every data to be written in a logical zone is structured within a logical transaction;

Logical Transaction := { l.z., f1/v1, f2/v2,. . . signature,date }

where f1/v1 stands for field_name and atomic typed value,
l.z. = logical zone number

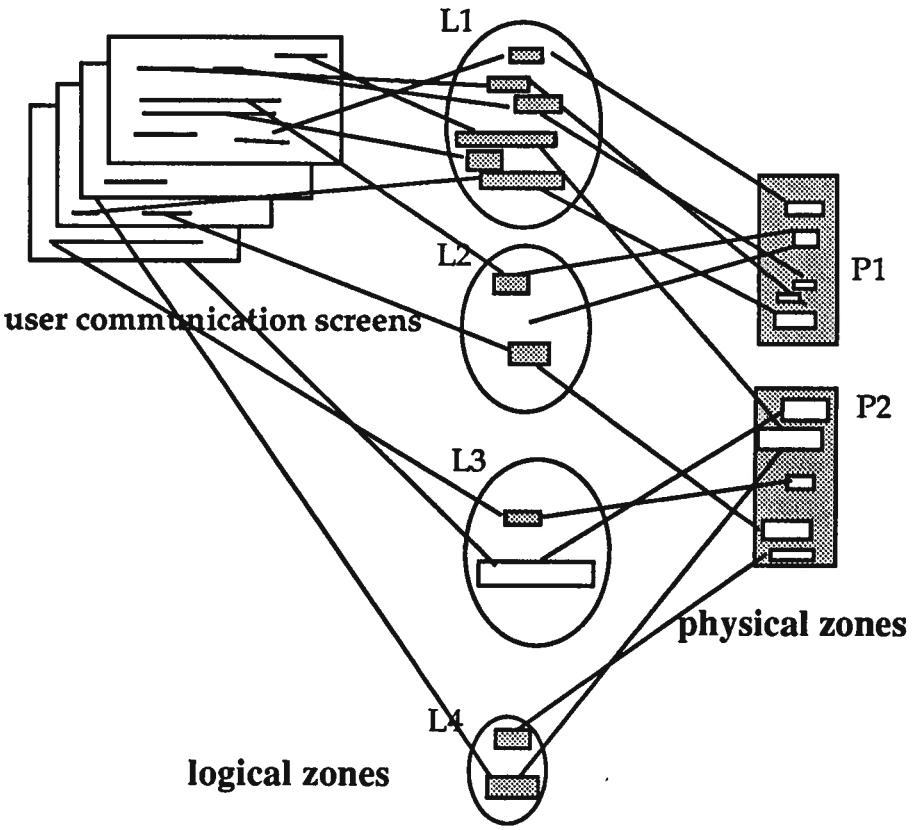
Physical zone (System Level)

A physical zone is made of data elements (from logical zones) sharing the same access rights for all user groups;

---> we could have approximatively 15 physical zones in the QPMR
A physical zone is implemented through allocation of physical blocks, as they may be configured in a given smart card technology.

Mapping between logical and physical zones

This mapping is implemented at the system level and a user application is not concerned with physical zones.



Critical technical issues:

- The unavoidable state of memory saturation: later, the better. . . [Ardouin 1990]

As we accumulate (strong system's constraint) medical data on the PMR without having any on-site deletion mechanism, a saturation will someday occurs.
Some strategies relevant to the PMR:

- Postponing:

using memory management and effective compression techniques;

- Expanding the PMR's memory:

Resolution saturation of memory by a new card by content abstracting and reissuing of a continuation card.

what is the probability of this event?
who is going to reissue the care card?
what is the frequency of this operation on a time scale?

- Non-stop service to users in spite of technological upgrades or breakthroughs

In a large scale implementation of the QPMR, the system will have its own dynamic and evolution over time ; it should cope with new information needs and new card technologies without any service interruption;

Part 2

Memory Allocation policies [Ardouin 1991]

- Fixed length static allocation (FLSA) :

- entire memory divided into blocks of fixed and identical size;
- all are allocated at issuing time.

2) Variable length static allocation (VLSA) :

- entire memory divided into blocks of fixed size;
- block size differs between zones;
- all are allocated at issuing time.

3) Fixed length dynamic allocation (FLDA) :

- entire memory divided into blocks of fixed and identical size;
- at issuing time, one block is allocated to each zone;
- further block dynamically allocated when needed.

4) Variable Length Dynamic Allocation (VLDA) :

- quite similar to FLDA;
- the size of each block may vary from zone to zone based on expected usage.

5) Dynamic Length Dynamic Allocation (DLDA)

- quite similar to VLDA;
- block size varies within a zone.

6) Dynamic allocation with zone increase (DAZI):

- a zone is allocated at issuing time with minimal space;
- each time a transaction is written in a zone, only the space needed will be contiguously allocated.

Saturation of a data zone

A potential saturation (PS) occurs when a zone cannot receive more data;

a final saturation (FS) occurs when a PS cannot be resolved by a given policy.

Saturation resolution policies

1) Erasing information within the same zone (ESZ)
---> may extend the card's life;

2) Erasing information in other zones (EOZ)
---> may give further extension to storage capacity;

3) Erasing information with zone shrinking (EZS)
---> may extend the card's life;

4) Disallocation of free space in any zone with reallocation (DFS)

5) Do nothing ---> final saturation

Simulation model

- An optimal design would maximize card life cycle.

- Life cycle depends mainly upon card usage.

- Card usage is characterized by number, type and size of logical transactions;

Model [Ardouin 1990]

The model has 12 parameters and generates transactions (medical, pharmaceutical and emergency) according to a Poisson's law.
Some parameters of the model:

memory space on the card

size of a zone

size of a transaction: min and max bits

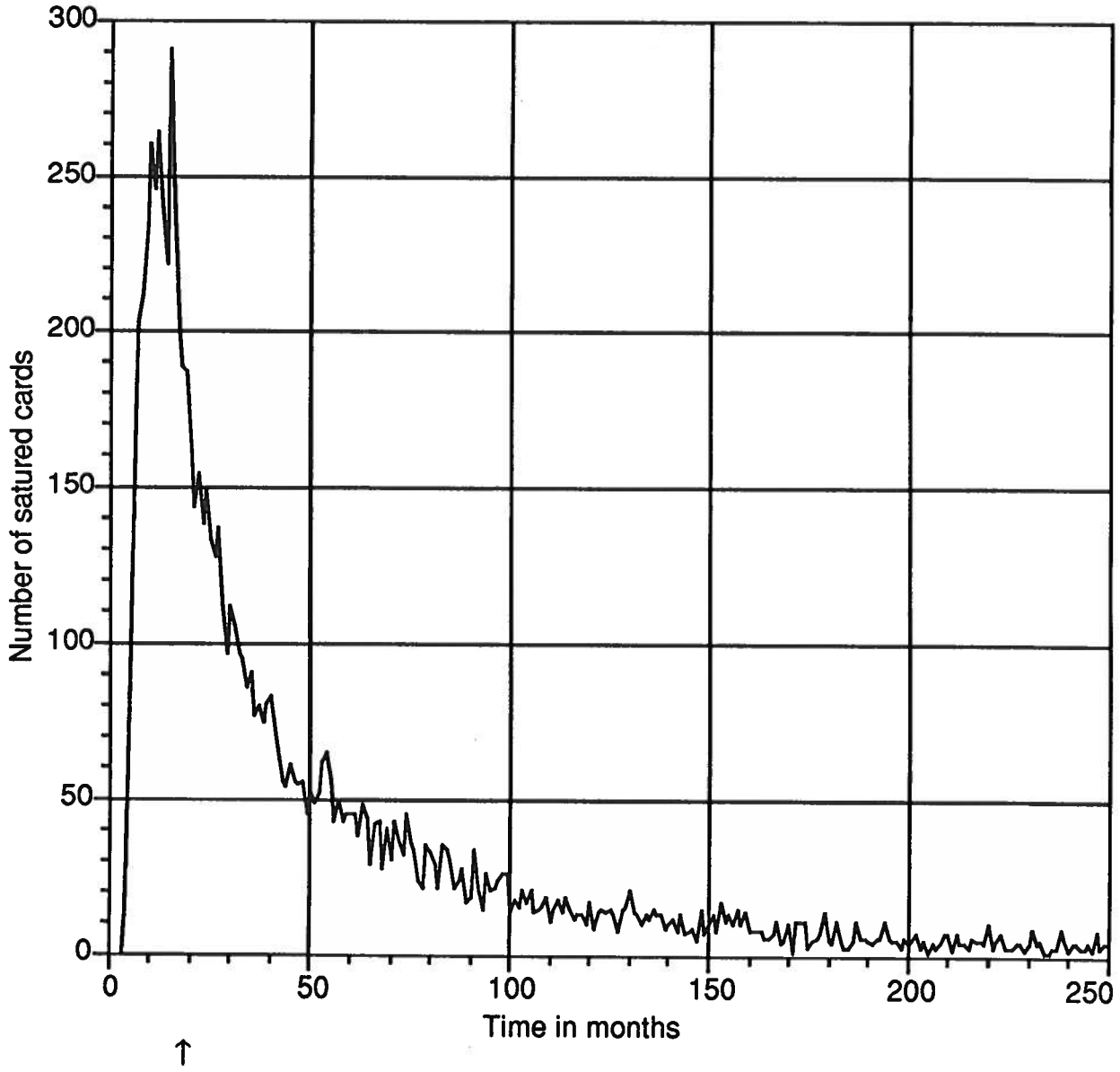
size of block descriptor

probability on the nature of a transaction: md, pharmacist, ...

memory management policy

saturation resolution policy

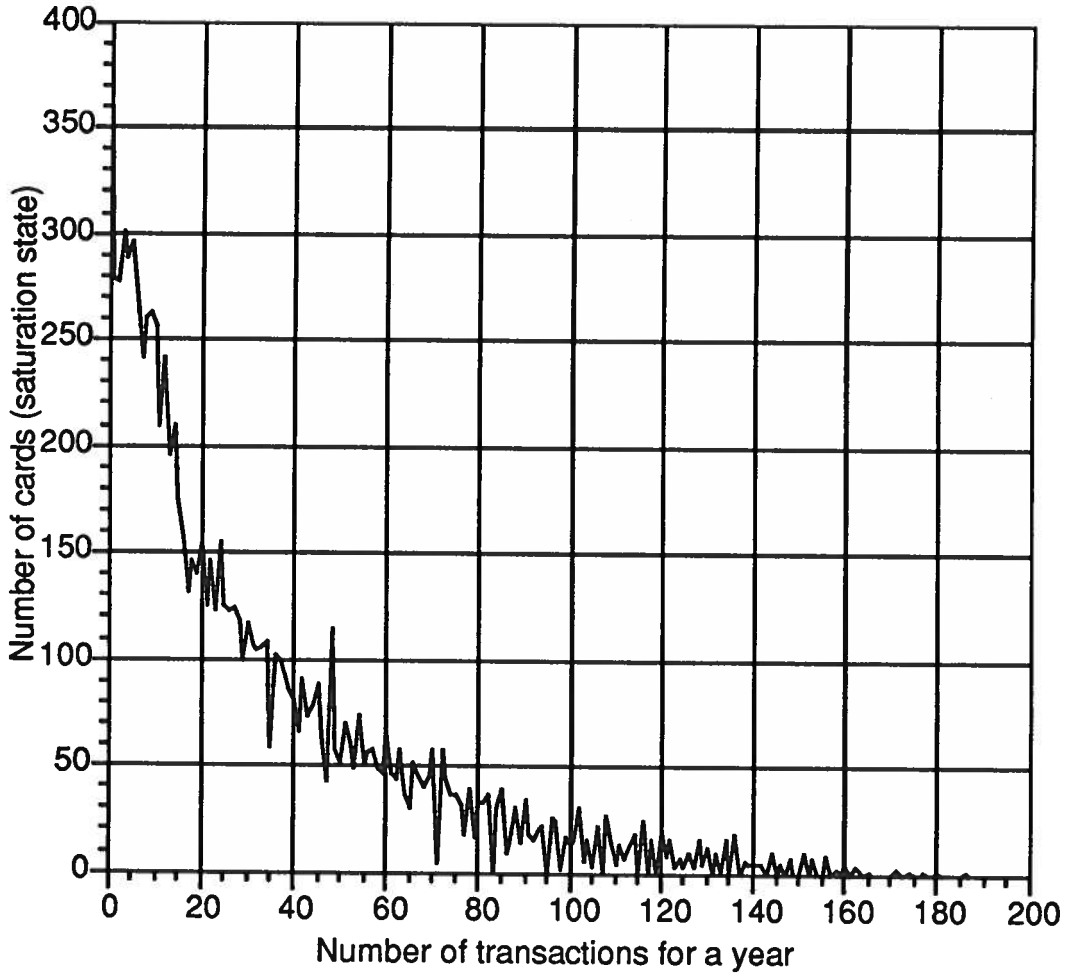
Saturation vs time



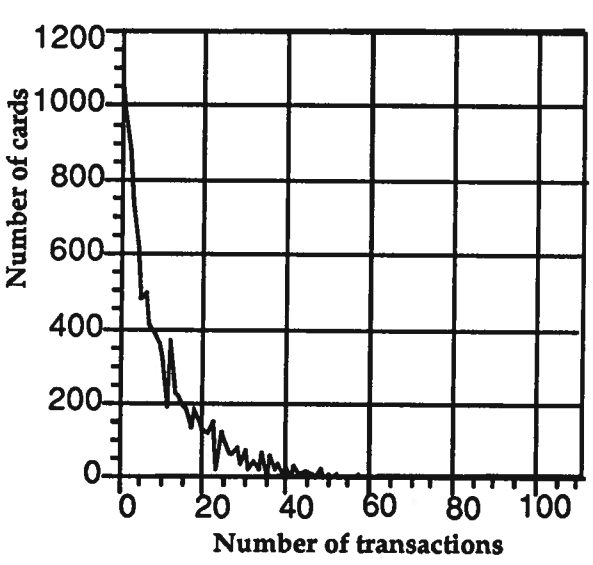
↑

VLDA: 32 Kbits
10 000 cards
no resolution of PS

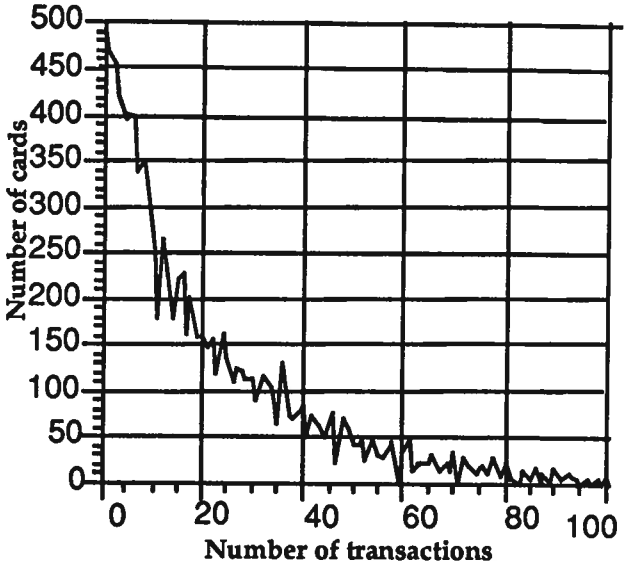
Distribution of cards over the number of transactions



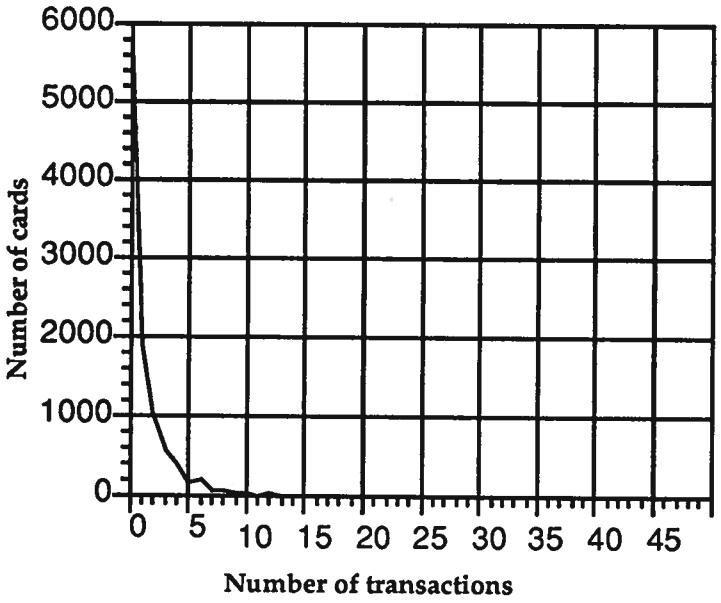
VLDA : 32 kbits
10 000 cards
no resolution of PS



Physician



Pharmacist



Emergency

VLDA: 32 Kbits
10 000 cards
no resolution of PS

Typical Results from Simulation

Effect of memory allocation and saturation resolution policies

Memory allocation policy	Saturation resolution policy	Life cycle (months)	
		For a 32 Kb card	For a 64 Kb card
VLSA	None	11,7 m.	30,7 m.
DAZI	None	15,8 m.	36,4 m.
VLDA	None	19,2 m.	39,0 m.
VLSA	ESZ	19,7 m.	39,5 m.
VLDA	ESZ	25,4 m.	49,7 m.
DAZI	ESH	30,2 m.	70,1 m.

Number of transactions in different zones at card saturation

Memory allocation policy	Number of transactions when saturation occurs (32 Kb card and no saturation resulution policy)		
	Emergency	Medication	Medical
VLSA	1,8 tr.	24,0 tr.	10,5 tr.
DAZI	2,1 tr.	33,1 tr.	15,4 tr.
VLDA	2,7 tr.	40,3 tr.	17,7 tr.

Effect of memory size on proportion of cards reaching saturation

Memory size	Proportion of cards reaching saturation within 18 months
32 K	30 %
64 K	8 %
128 K	< 0.1 %

Some comments on these results:

- The simulation indicates that a problematic situation exists and the proposed system should take somewhat into consideration these simulation results;

- Better results would be available soon based on real data obtained from the RAMQ (1989-1991);

- The life cycle seems to be long enough to support the pilot project;

- The final saturation could be resolved by:

  - an adequate memory allocation policy and

  - centrally issuing a continuation card.

Part 4

Compression techniques used in the PMR [Zaïane 1991]

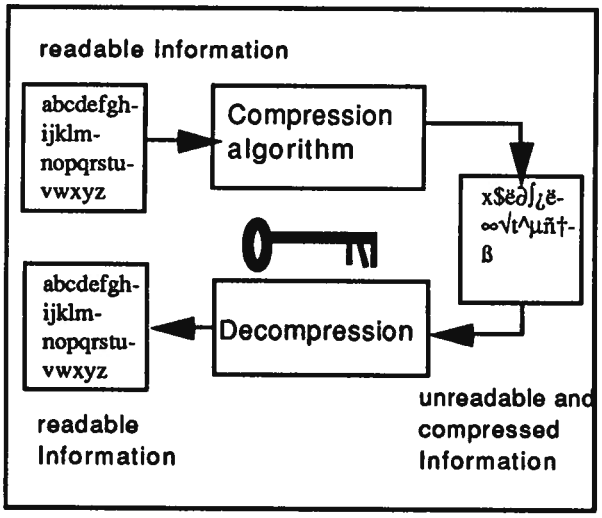
Some advantages in using compression techniques:

- To save memory space: good compression may further delay the saturation state in a physical zone;

---> many algorithms available which give various compression factors depending on input information

- To decrease the communication time on serial line: may be useful to get on-line access to laboratory results;

- to improve security by reducing redundancy in the information;



Text compression reversible algorithms

Many of them are available [Bell 1990]; our first choice is composed of the following coding classes (assuming a noiseless channel):

- Huffman coding
- Lempel, Ziv, Welch algorithm
- Arithmetic coding
- LZHUF algorithm

Text files used to measure the performance of compression techniques:

- random binary digits file
- pre-coded medical file with minimal redundancy
- pre-coded medical file with redundancy
- free-text medical file

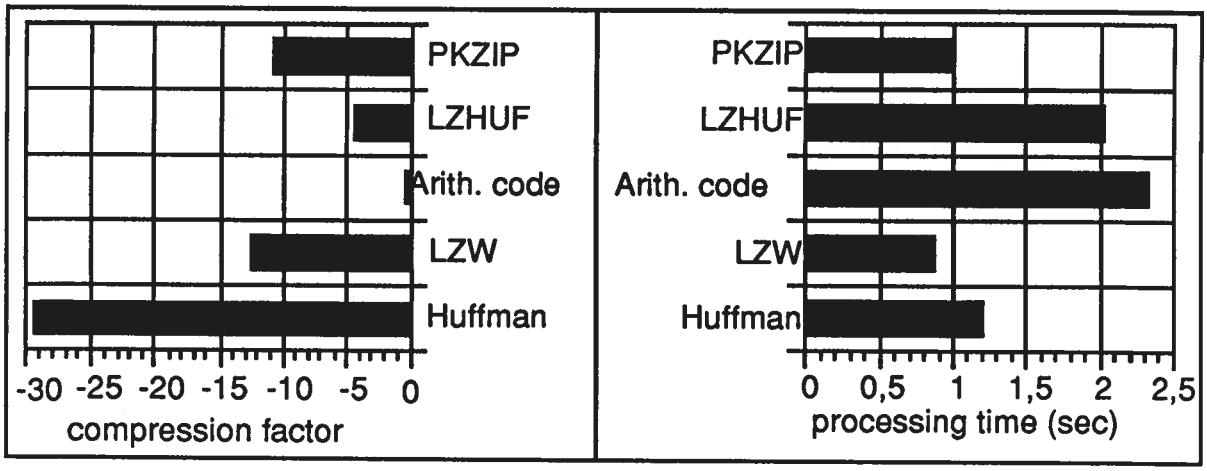
The compression factor used to compare the results is defined as follow:

Compression factor = (Li - Lc) * 100 / Li

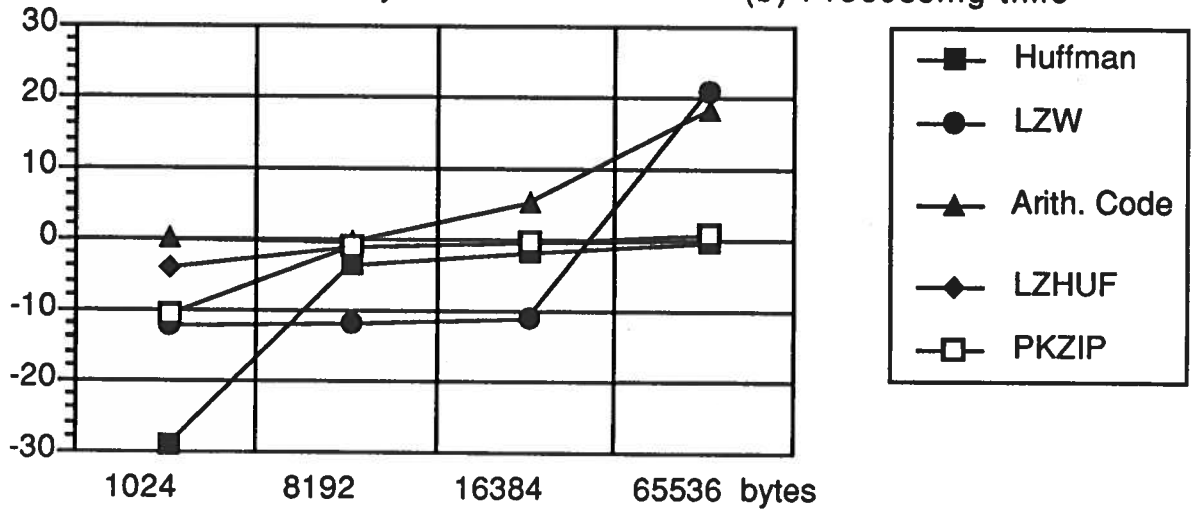
Li = length of the plain text Lc = length of compressed text

A positive CF means saving space on the card memory.

File of random binary digits: L= 1024 bytes



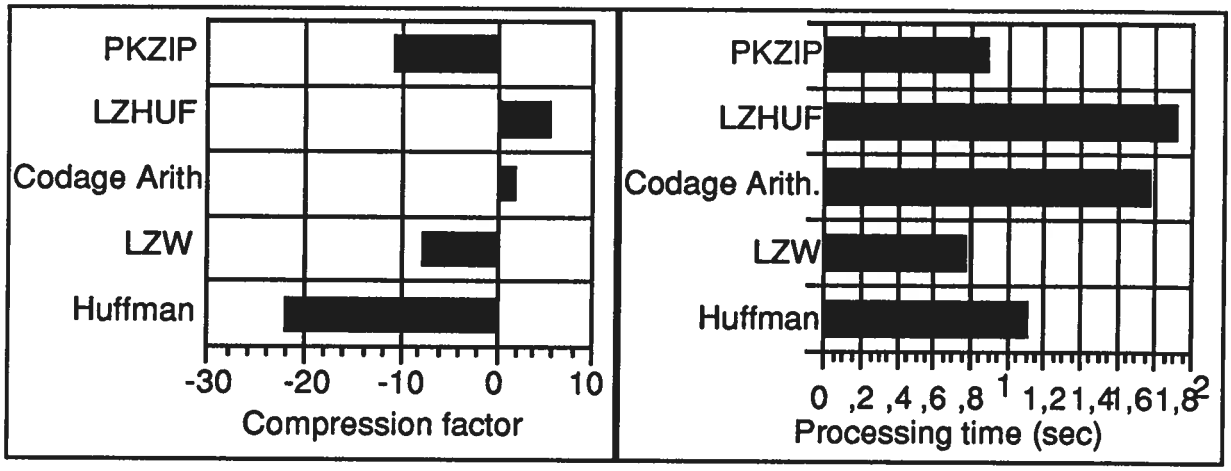
(a) Buffer of 1024 bytes (b) Processing time

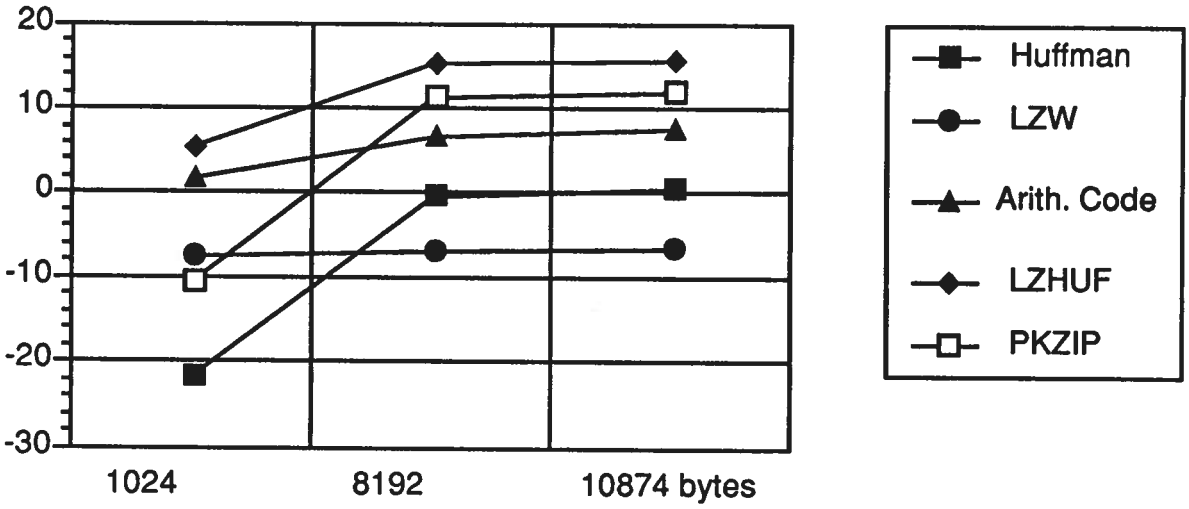


(c)Compression factor versus size of plain text

Space is increased by Huffman algorithm: 30% of space for a processing time of 1.5 sec.

File of pre-coded medical records (L= 1024 bytes)

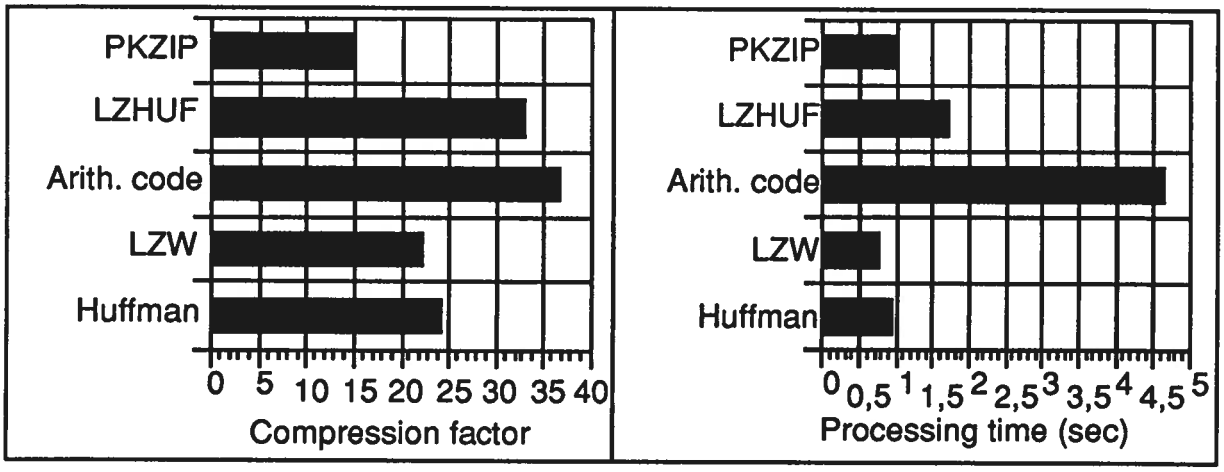


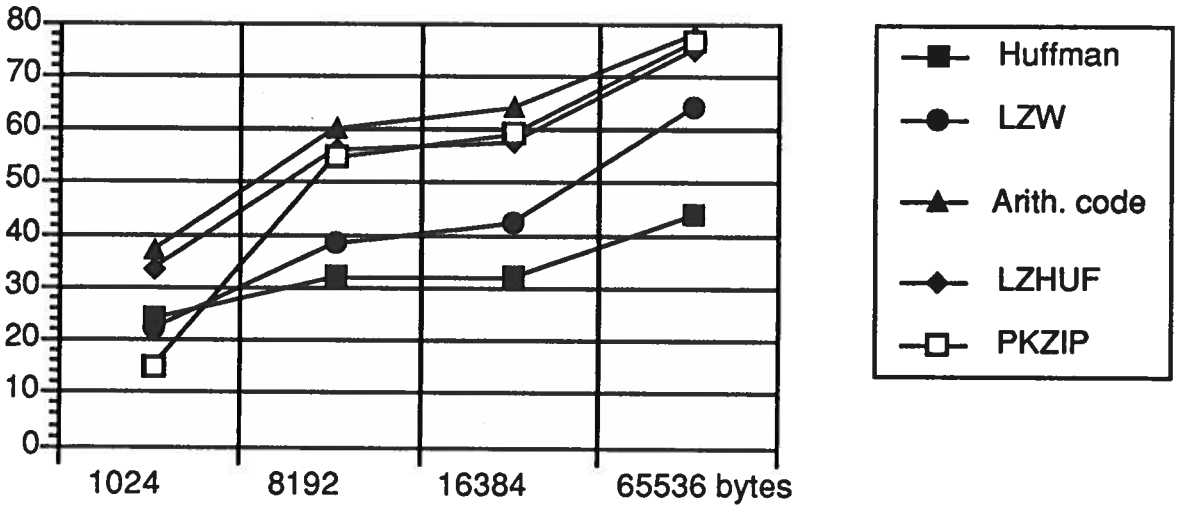


(c) Compression factor versus size of text

With a file of pre-coded medical records, much compression has been done manually and the LZHUF algorithm is still able to compress (6%) the information to be stored in a physical zone.

File of medical records in free text form (L= 1024 bytes)





(c) Compression factor versus size of text

With a file of real medical records in free text form, the LZHUF does a good compression (35%) within a very short period (1,5 sec).

Conclusions

The design of a smart card based software system imposed some strict constraints which call for new ways of managing and storing medical data on the car. Within the framework of smart card technology which provide very good security mechanisms, we propose some ideas to make a better use of this technology:

1- Compression techniques appear as a valuable tool to further delay the saturation state of a card;

2- Algorithm LZHUF is the best buy: good compression factor and small processing time;

3- With the imposed constraints to a PMR, memory management policy should be considered (if implementation is feasible) with a given smart card;

4- The two-layered shell is a good structure to immune applications with regard to major upgrades at node level and to allow, eventualy the use of various cards in the network.

5- New technologies could be usefull to store more information in the PMR, providing they do that in a way as much secure as it is with the smart card.

* * *

Acknowledgements

This work has evolved from a project funded by the Régie de l'Assurance Maladie du Québec (RAMQ). Members of the pluridisciplinary research group have contibuted to this work by providing various ideas and making constructive comments, namely Eric Bellavance, Guy Girard, Christian Boudreault, Jocelyn Bérubé, Jean-Paul Fortin, Suzanne Hamelin, André Hémond, Guy Lavoie, Marc St-Pierre, Luc Tremblay and Alain Vanasse.

* * *

References

Ardouin 1990 P. Ardouin, A. Gamache and al **Effects of memory saturation in the design of a portable medical record,** Proceedings of the Third Global Conference on Patient Cards, March 1991, Spain, 5p.

Ardouin 1991 A. Gamache, P. Ardouin **A Formal Model for Analysis of Memory Allocation and Saturation in the Design of a Smart Card Based System,** Proceedings of SCAT-91, Washington, May 1991, p.134-145.

Bell 1990 Bell T., Cleary, J. and Witten I.H., **Text Compression,** Prentice Hall Advanced Reference Series, ISBN 0-13-911991-4, 1990

Cantin 1990 Cantin, Rejean, **Projet Carte-Santé du Québec,** Conférence à l'Expo-Congrès International des Technologies d'Information, Montrèal, septembre 91

Cantin 1991 Cantin, Réjean **Conférence au Séminaire international sur les applications de la carte à mémoire,** Stéria Canada, Montréal, mai 1990.

Durant 1990 Durant, Pierre **Un serveur généralisé de carte à microprocesseur,** Mémoire de maîtrise, Université Laval, 1991.

gamache 1990 A. Gamache, P. Ardouin et al **Caractéristiques systémiques et techniques d'une carte-santé réalisée avec la carte intelligente,** Actes du Colloque de l'Université Laval sur les cartes Intelligentes, Septembre 1990, 27p.

Zaïane 1991 Zaïane, Rachid, **L'accès logique aux données d'un dossier médical géré par une carte à microprocesseur,** Mémoire de maîtrise, Département d'informatique, Université Laval, 1991.