Please note that an image is missing from this document

Secure banking application for broadcast data systems

P. Shiel (Trintech International)

The enormous growth in the use of "plastic money" has brought with it a need for fast, cost-effective methods for combatting fraud. A new application of the Radio Data System provided by Radio Telefis Eireann, means users of lost or stolen credit cards can be caught "red-handed", without the need for costly and time-consuming verification of every transaction by telephone.

The system uses the RDS channel to broadcast continuously up-dated lists of suspect card numbers to cash-register systems in shops, super-markets and other business premises.

1. Introduction

Radio Telefis Eireann (RTE) has incorporated data channels in its VHF/FM broadcasts for many years. Initially, using the MBS system, applications were limited to internal tasks and in particular as a paging service for the RTE's remote engineering and maintenance crews. With the advent of the Radio Data System (RDS), which came into service in Ireland in 1984, all paging services were transferred from MBS.

It was soon recognised that there was considerable scope within the RDS channel for various commercial applications. Commercial partners were therefore sought and one of these, Trintech International Limited, has developed a new application for use via the RDS system. The joint development has lead to the introduction of a secure banking application involving the transmission, via RDS, of the numbers of lost or stolen credit cards - known familiarly as "hot cards".

The major impetus for this development has come from the market-place, where there is need to reduce the operational cost of a secure credit card sales system. The banking community has many options in this area, which vary significantly in

Original language: English
Manuscript received 20/7/92.

their set-up costs, running costs and degree of security against fraud. The traditional solutions have relied heavily on the public switched telephone network (PSTN) for on-line authorisation of each transaction by reference to a central "hot card file". This has reduced fraud, but has substantially increased the costs since each telephone call must be paid for by the banks or businesses.

The principal novel feature of the new system is that the content of the central hot card file is distributed nationwide to all business premises included in the system. The cash register systems operated by those businesses, which may comprise one or more electronic funds transfer point of sales (EFTPoS) terminals, can then make local checks for suspect cards. Depending on the result of the local check, the public switched data network (PSDN) can be used as appropriate, thus maintaining a high level of security but substantially reducing the telephony charges. The instantaneous up-dating of the data held in all EFTPoS terminals is the cornerstone of this system, and the RDS system has proved an effective solution for this point-to-multipoint transmission requirement.

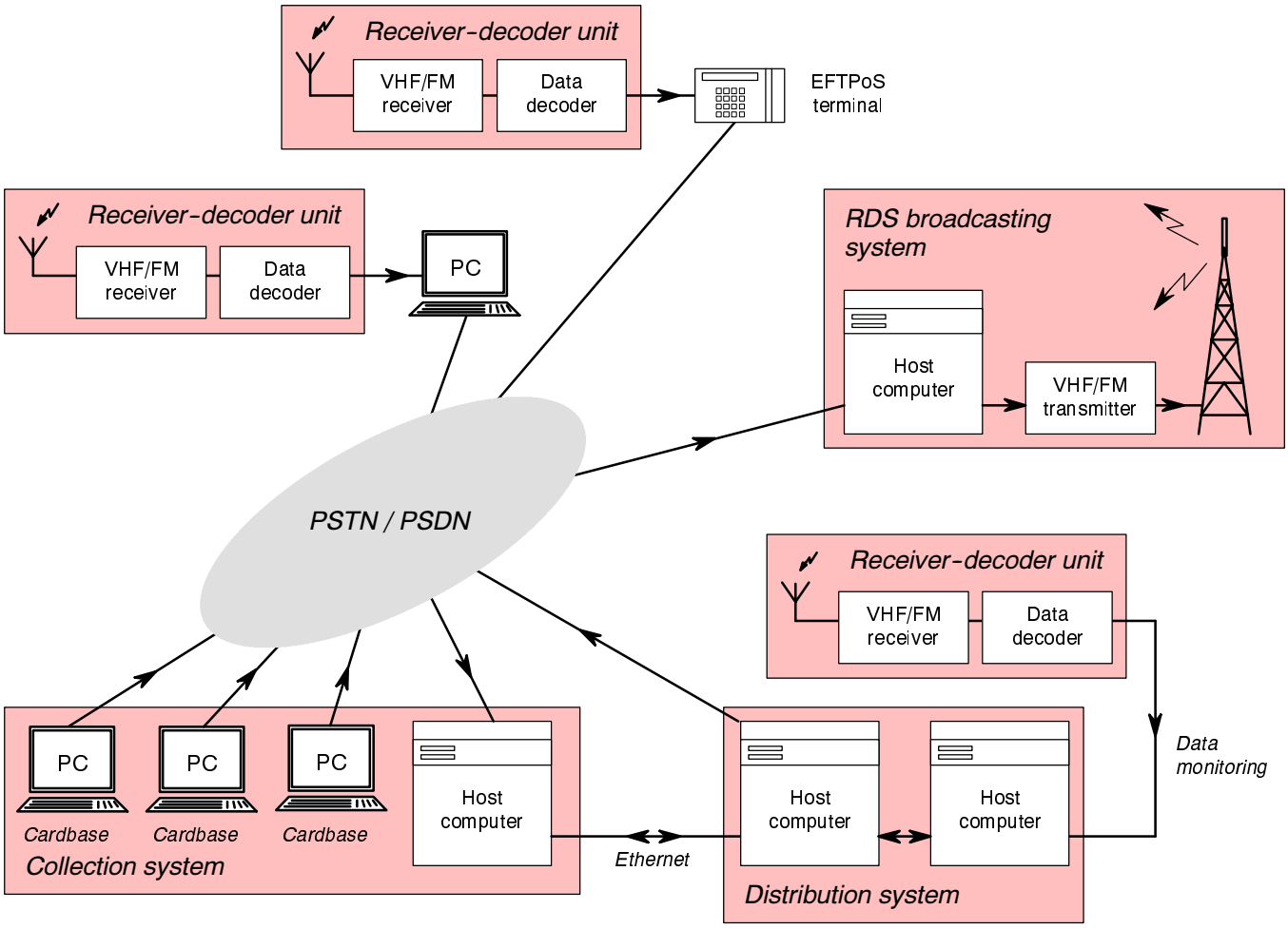
2. System architecture

The overall system architecture includes several elements ranging from high-level Unix data collection and distribution software to RDS transmission multiplexers and RDS scanning receivers. The system can be considered in four parts, shown in *Fig. 1* and described below.

2.1. Data collection

Each bank which participates in the system is able to contribute to the central hot card file. The bank uses the "Cardbase" software package running on a personal computer to enter, sort and store the latest hot card numbers brought to its attention by card owners. The assembled data are then forwarded to the collection system, as soon as the numbers have been entered. The collection system, which will run on any Unix platform conforming to the XOPEN standard, then sends the hot card file up-dates to the distribution system.

Figure 1
System architecture



The collector also responds directly to requests from any EFTPoS terminals which require a hot card up-date via the PSDN rather than via the RDS channel.

2.2. Distribution

The distribution system is also based on Unix technology, but is physically separate from the collection system. The two systems can be connected serially or via an Ethernet local area network (LAN), according to the volume of data to be transferred. The distribution system carries out further hot card sorting and passes the data to the host computer installed at RTE. It also maintains a log of all data sent for RDS transmission, and of RDS data received from a local VHF/FM transmitter; in this way the broadcast transmission loop is closed and integrity of the data transmission is constantly monitored.

2.3. Transmission

The transmission system consists of a multi-tasking front-end processor which concentrates the incoming data for RDS transmission. The hot card file data are transmitted several times each hour in a reserved information group (6A) of the RDS data multiplex, and the complete RDS signal is broadcast in the normal way.

2.4. Receiver-decoder

The final element in the loop is the Trintech RDS receiver which can be integrated as part of an EFTPoS terminal in any business premises where the RDS signal can be received satisfactorily. The receiver decodes the hot card file and either sends the data to a host computer or EFTPoS terminal via a serial data link, or stores them in its internal memory. If the receiver maintains the local hot card file internally, it can be interrogated by the host computer (or any of the EFTPoS terminals) to verify the validity of any card. If the card number is present in the hot card file, the host computer (or EFTPoS terminal) treats the card as suspect and then seeks positive authorisation via the PSTN or PSDN, as appropriate.

3. Hardware

3.1. Data collection and distribution

The central Unix data collection and distribution systems can run on a variety of hardware platforms. These systems are completely unattended, but they must provide 100% availability for incoming hot card up-dates from the Cardbase packages. Data security and system availability are discussed in more detail in *Section 4*.

3.2. Receiver-decoder

3.2.1. Hardware

The receiver-decoder unit installed at the business premises includes all the necessary functions for a complete RDS monitoring and data storage device. The standard configuration comprises:

- an antenna (quarter-wave whip or half-wave dipole, depending on the reception conditions);
- the receiver-decoder unit (RDU);
- a host device (computer or EFTPoS terminal, connected via a serial data link).

The RDU can also be connected to an RS 422 LAN for multi-EFTPoS terminal installations, such as are found in supermarkets and other large stores. *Fig. 2* shows some typical options for installations in business premises.

The radio-frequency sections of the RDS receiver are of basically conventional design, but special attention has been given to achieving high sensitivity with the result that error-free operation is possible with RF input levels as low as 20 dBμV. Receiver tuning (automatic FM band-scanning and channel pre-selection) is controlled by the RDU software

3.2.2. Software

The data and clock signals delivered by the RDS decoder are fed to a microprocessor-controlled data decoding system whose software is very rich in functionality. This has been achieved by making all the operating parameters software-loadable during installation. In addition, to maximise

Patrick Shiel *is Technical Director of Trintech International (based in Dublin) where his responsibilities include the overall strategic planning of new products and markets.*

Mr. Shiel was educated at Trinity College Dublin from which he holds a first class honours degree in engineering and the University of California, Berkeley. Before joining Trintech, Mr. Shiel spent considerable time in the USA, primarily in the large system architectural design area in which he holds patents for his work.

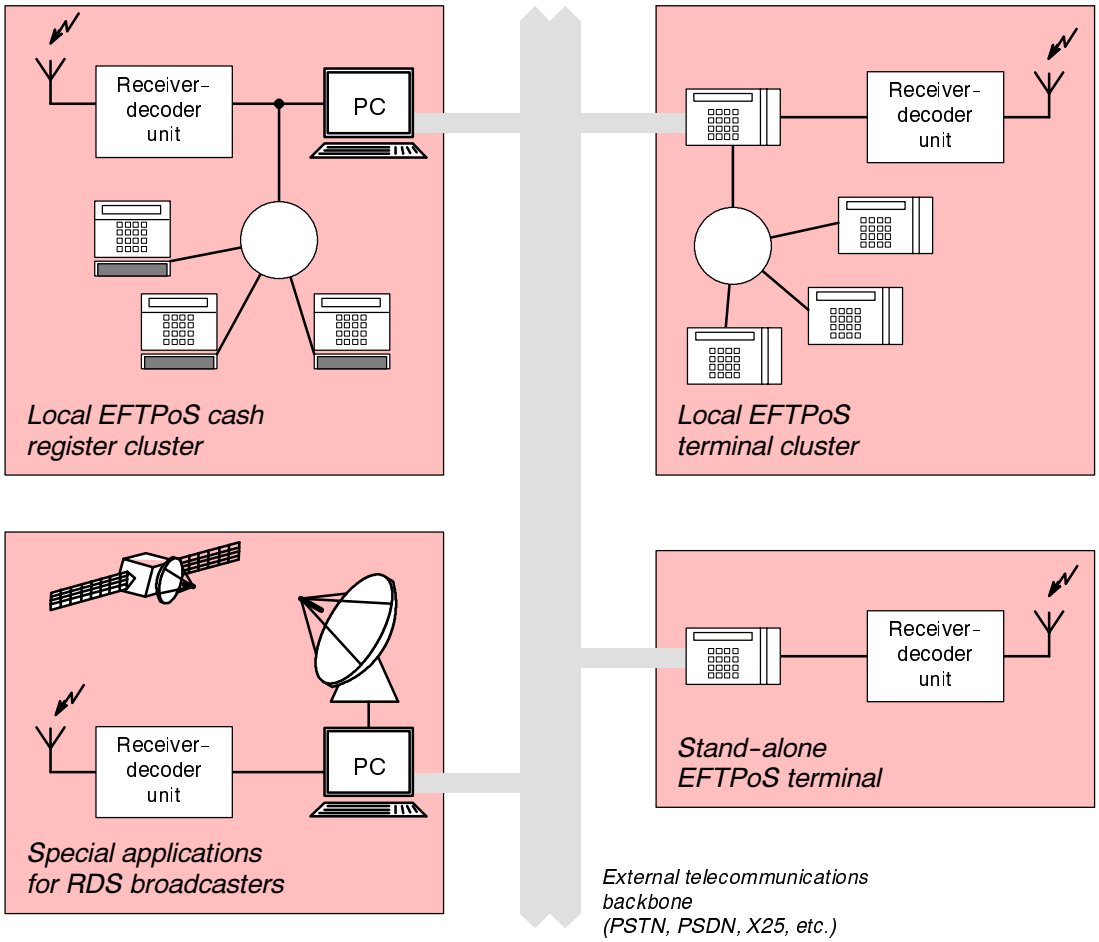


Figure 2
Possible equipment configurations in business premises

flexibility, the parameters can be re-loaded, or changed "on the fly" by a host computer, EFTPoS terminal or remote computer connected via modem.

The decoder can detect many error conditions as they arise, including disconnection of the antenna, loss of synchronization to the RDS data-stream, power supply problems, etc. Such error conditions can pose a security threat to the installed system, so the RDU can initiate a warning telephone call to a responsible person.

Other software functions include control of VHF/FM band-scanning, system commands (e.g. timing of hot file down-loading, choice of storage options, ...), hot card file commands (clearing out-of-date data, loading new data, ...) and basic operational tasks such as the verification of card numbers and internal telephone directory maintenance.

In normal operation, the decoder searches the RDS data-stream for data carried in RDS Group 6A and applies special error detection and correction routines. With 10 bits of error-correction code for each 16 data bits, the probability of detecting and correcting all one and two-bit errors is greater than 99.9997%.

Banking organizations require a system which can handle a maximum number of hot card numbers safely and rapidly, so data storage and transmission capacity is a critical element in the hot card system in general and, more especially, in the RDU where memory may be limited. For this reason, Trintech have developed a compression technique which takes the standard 16-digit credit card account number and compresses this to seven bits. These seven bits are rarely contiguous in memory, so high-speed mapping algorithms are used for data insertion and retrieval. With the chosen compression technique, over 980,000 card numbers can be stored in an RDU with no more than 1 Mbyte of memory.

If the RDU is requested to forward all hot card numbers to a host device, the data are sent uncompressed via an RS232C or RS422 serial interface. This enables even the simplest host device to decode and manipulate the hot card data as required.

4. Data integrity

The system described here must perform to the very highest standards of fault tolerance because of the very sensitive nature of the data being transferred. For this reason, a "hot back-up" is provided for every stage of the long data transfer chain where this is feasible.

Data storage on any of the computer systems is triplicated on disk. Under normal operating conditions only the primary copy is used, but if an error condition is detected within the primary databases all three copies are polled to determine which of them contains the data errors. A shadow database is also held on removeable media to guard against complete system failure.

The collector and distribution systems maintain not only shadow database copies on the individual disks, but each computer also keeps an additional copy of the other system's disk. If one Unix system should fail, the other will detect this condition and take over the functions of the failing system. Each of these systems can make an RDS radio-paging call to a service engineer at any time of day or night.

The RDU is the part of the overall system which requires the highest level of guaranteed data integrity, so the RDU is designed to be self-monitoring. It can raise an alarm by informing the attached computer of EFTPoS terminal of any difficulties it encounters. The EFTPoS then initiates a phone call, at the request of the RDU and, once the connection is established, control of the PSTN (or PSDN) data channel is passed directly to the RDU which sends a message to the collector system for logging. Fault analysis is carried out by the collector which can initiate an RDS radio-paging call to the service personnel if it decides it cannot correct the fault itself. Experience with the system to date shows that almost 98% of all operational problems can be corrected without any intervention by service personnel.

5. Conclusions

The hot card file distribution system described here has been installed in many locations in Ireland and the United States of America (where MBS coding is used instead of RDS). There has been a very significant decrease in credit card fraud and - more importantly - a significant increase in the recovery of stolen cards.

All the data-processing parts of the system have been designed to work in conjunction with any data broadcasting channel; it is not restricted to use with the Radio Data System. Other transmission options may include satellite services, microwave terrestrial broadcast systems, teletext or other forms of FM transmission outside the conventional broadcast bands.

The system is designed to permit easy expansion of all sub-systems. At present 10% of the available capacity is used and there is sufficient spare capacity to cater for the expected growth in the credit card industry, particularly over the next five years. A steady expansion of the collection, distribution and transmission systems will be implemented, within the existing system architecture.

ITU on-line

An electronic document distribution service providing remote access to ITU documents came into operation early in November 1992.

The database service, known as TELEDOC, is intended to provide fast and timely access to the world telecommunications and networking community, and already contains a wide variety of ITU documents: administrative texts, lists of contributions to the CCIR and CCIR Study Groups, lists of CCITT Reports and Recommendations, summaries of new or revised CCITT Recommendations, meeting schedules of the CCIR and CCITT and related information. The database will be expanded and, for example, by early 1993 it will contain the full texts of all new or revised CCITT Recommendations.

TELEDOC is based on an X.400 document server which processes requests sent in by electronic mail. The auto-answering mailbox system accepts messages from the two most-widely used E-mail systems, X.400 and Internet. Users who do not have direct access to either of these E-mail systems can use one of the many gateway services available from service providers.

A thorny problem in any document distribution system of this sort is the formatting of the documents; the ITU plans to make documents available in a range of formats including ASCII, Microsoft RTF, Word for Windows, PostScript and CCITT ODA/ODIF.

ITU