1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6-8, 1984, Zurich, Switzerland, Swiss Federal Institute of Technology, Proceedings IEEE Catalog Nr. 84CH1998-4, 183-190

A switched/broadcast ISDN to decrease user observability

Andreas Pfitzmann

Institut für Informatik IV, Universität Karlsruhe,
Postfach 6380, D 7500 Karlsruhe 1, West Germany

ABSTRACT

In usual networks user behavior could easily be observed by traffic analysis, even if the users employ end-to-end encryption. Hence a switching/broadcast network structure (SBNS) is derived, which decreases user observability.
The SBNS proposal is

1. physically based on cheap and powerful microelectronics (e. g. personal computers) and on the enormous bandwidth and inherent broadcast facility of local networks and
2. logically based on the generation of random numbers and keys of a public key cryptosystem.

The backbone of the SBNS proposal is a conventional circuit or packet switched ISDN. The terminals of the switched ISDN are gateways. Each gateway masters a local two-way broadcast network which connects the user stations of a user group. Implementations of local two-way broadcast networks are discussed and protocols derived, which together can hide the sender and receiver of a message but enable the generation of untraceable return addresses, digital signatures and billing.
Costs, fault tolerance and protection against fraud are discussed.
It is shown, how patterns in time of the message traffic can be reduced. Otherwise, patterns in time could be used to monitor user behavior, too.
At last, the SBNS is compared with the only other known solution to the traffic analysis problem. The other solution is found to be too costly in terms of required bandwidth.

1. INTRODUCTION

> With the development of television,
> and the technical advance which
> made it possible to receive and transmit
> simultaneously on the same instrument,
> private life came to an end.
>
> George Orwell

In practically all proposed or realized public two way communication networks user stations can easily be identified at the Physical-, Data Link- or Network Layer [9]. Therefore the public network (or an intruder) could easily monitor when, how much and with which other instance a user of the public network is communicating, even if end-to-end encryption is used.
When more and more human-human or human-computer communication uses public networks, the possibility of monitoring may become unacceptable. Hence a switching/broadcast network structure (SBNS) is derived in [15], which decreases user observability.
The SBNS proposal is

1. physically based on cheap and powerful microelectronics (e. g. personal computers) and on the inherent broadcast facility of local networks and, if it is used as ISDN, on the enormous bandwidth of coaxial cables [10] and optical fibers [1] and
2. logically based on the generation of random numbers and keys of a public key cryptosystem [4, 6, 12, 26].

2. NOTATION

ke public key used for encipherment (and for checking signatures) in a (some, e. g. [19]) public key cryptosystem(s).

kd private key used for decipherment (and signature) in a (some) public key cryptosystem(s). kd is sometimes called secret key instead of private key.

ke(M) denotes a message M enciphered with ke. M is augmented with a random bit string of appropriate length to reduce the probability to guess M and verify the guess by enciphering M with the publicly known public key ke. For the sake of compactness, the notation hides the random bit string.

kd(ke(M)) = M is the property needed in this paper.

ke(kd(M)) = M holds in some public key cryptosystems and can be used for digital signatures.

3. THE SWITCHING/BROADCAST NETWORK STRUCTURE

3.1 The physical structure

The backbone of the SBNS proposal is a conventional circuit or packet switched integrated services digital network (ISDN). For the sake of clarity, only one switching-center is shown in figure 1.
The terminals of the switched ISDN are gateways. Each gateway masters a local two-way broadcast network. Each two-way broadcast network connects the user stations of a user group. The population of a city district or a building may form a user group, the employees of a company, too.

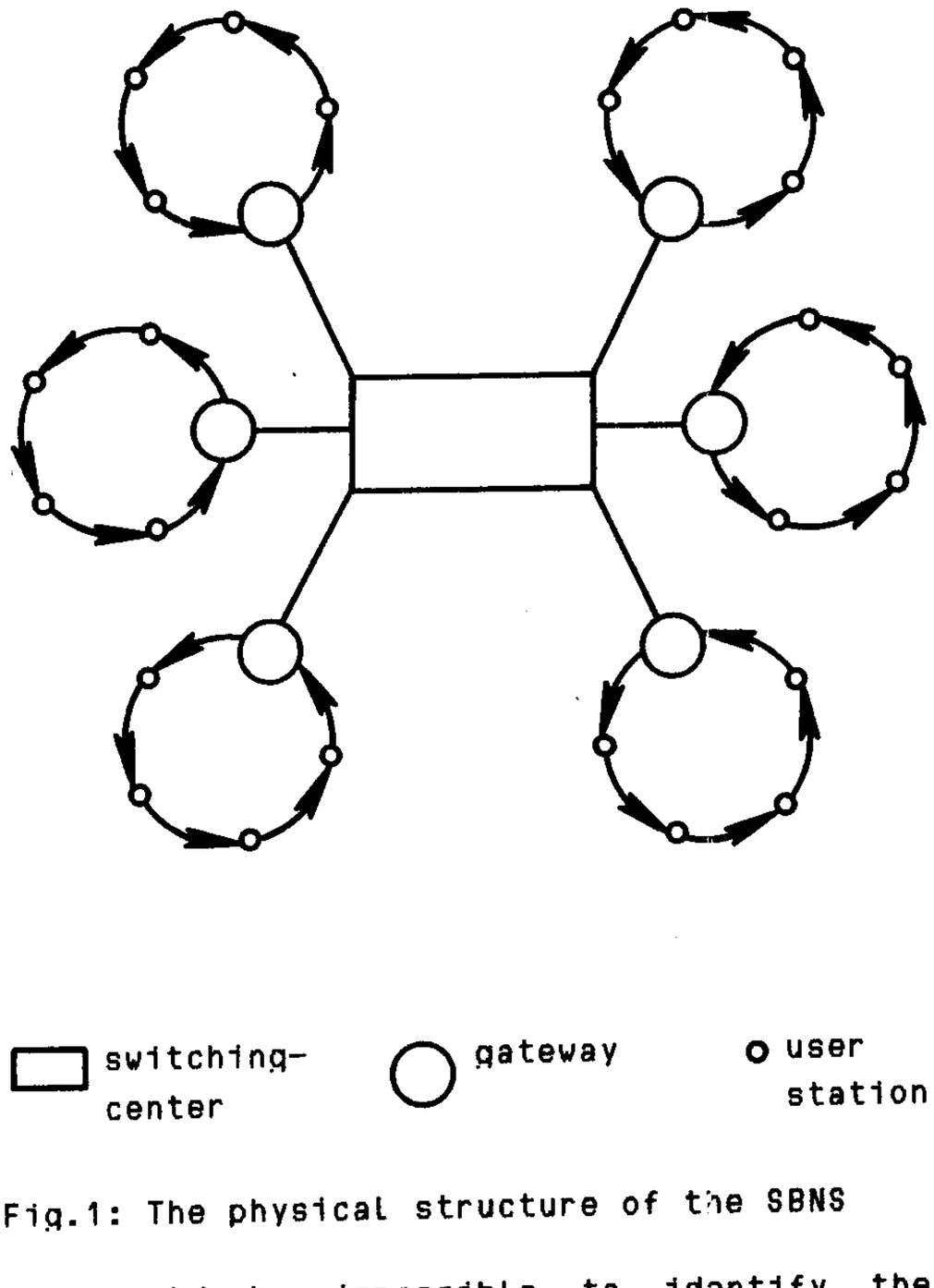


Fig.1: The physical structure of the SBNS

It should be impossible to identify the sender or receiver of a message in the local two-way broadcast networks by access to the local network at any single point.
If the local two-way broadcast network is implemented as a bus, the user stations at the ends can be identified as senders by tapping the bus between them and the rest of the user stations and monitoring the direction of signal flow. If the local two-way broadcast network is implemented as a loop and every sender removes the messages he sent after one trip around the loop and a random access protocol is used, there are no possibilities to determine the sender or receiver of a message [16]. Appropriate random access protocols for a loop are empty-slot (Pierce loop) or register insertion (delay insertion loop) [23, 24, 27]. In a token ring (Newell loop), and in its derivates, too, the sender of a message can be identified if all stations in the loop transmit a message.
Thus a Pierce loop or a register-insertion loop is the favorite solution.
For further discussion on bus versus loop see [20].

The cable run of the loop should make tapping the loop before and behind a user station as difficult as possible. E. g., in a house divided into several flats, the loop should connect the flats directly.

3.2 Organization and Generation of Addresses

The addresses of user stations in a SBNS are composed of 2 parts,which together are enciphered with a fixed public key of the switching-center.

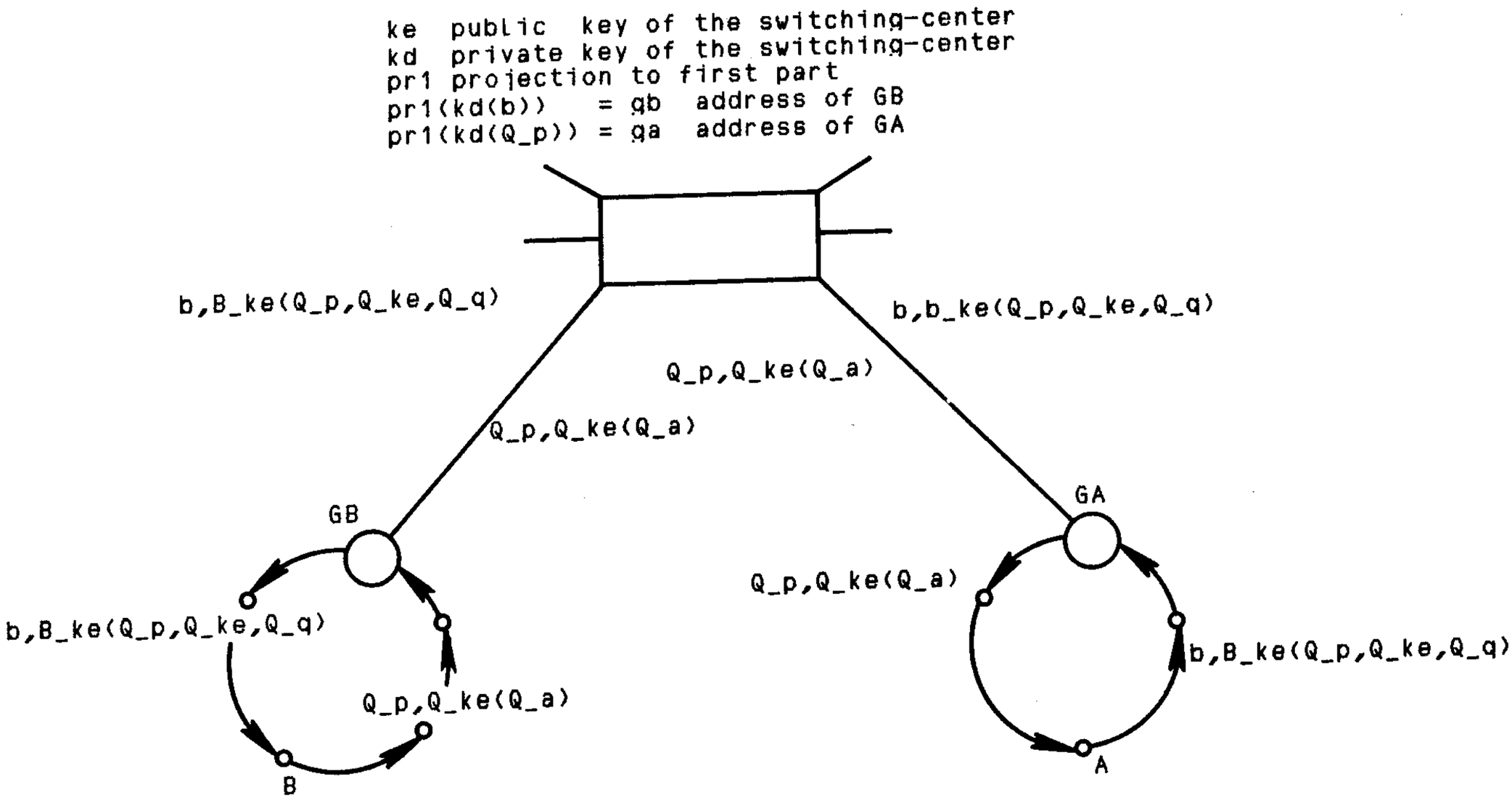
1) The first part is a logical address of a gateway. A gateway may have several different but fixed logical addresses. The logical addresses of a gateway are only known to the switching-center and to the user stations connected with the gateway by the two-way broadcast network.
2) The second part is a pseudonym of a user station. Each user station may have several different pseudonyms. Pseudonyms may be created and destroyed by each user station.

For every address in a SBNS, there exists a corresponding public key ke. All messages to an address will be enciphered with the corresponding public key ke. The receiver holding the address knows the private key kd corresponding to ke and deciphers all messages with the appropriate private key kd. One address with the corresponding public key of every user (who likes this) is published in a roster of public addresses of user stations. The roster of public addresses must be safeguarded against manipulation [16].
Besides or instead of a public address a user station may create private addresses with corresponding public keys, which the user may pass to friends, business partners

and so on.
Private addresses with corresponding public keys which he uses only once, are called untraceable_return_addresses. Everybody else and especially the switching-centers, gateways and other user stations cannot correlate untraceable return addresses with user stations.

3.3 The logical operation

The logical operation of the SBNS is demonstrated by an example. To keep the example easy to understand, only one switching-center is shown in figure 2.
A user at user station A wants to get information out of a database B. Thus he wants to send B a question Q_q.
A knows a logical address ga of its gateway GA and the public key ke of the switching-center. A also knows an address b and the corresponding public key B_ke of B, which he may have looked up in the roster of public addresses.
In its idle time, A already generated a random number Q_n using the algorithm presented in [22] or using a physical random number generator. A used Q_n as a pseudonym to compute a private address Q_p = ke(ga,Q_n). A also generated a public key Q_ke and a corresponding private key Q_kd. Q_p,Q_ke form an untraceable return address which even avoids an anonymous recognition of A based on a fixed address or a fixed public key.
A uses B_ke to encipher Q_p, Q_ke and Q_q. A sends b,B_ke(Q_p,Q_ke,Q_q) to its gateway.
The gateway GA of A sends the message to the switching-center.
The switching-center deciphers the address b of B and splits it into the address gb of the gateway GB of B and a pseudonym of B. The switching-center uses gb to send the message to the gateway GB of B.
The gateway GB of B broadcasts the received message.



b address of B
B_ke public key corresponding to b
B_kd private key corresponding to b
Q_p
Q_ke
Q_q
Q_a answer to Q_q

ke
ga logical address of the gateway GA
b address of B
B_ke
Q_n random number chosen for Q
Q_p = ke(ga,Q_n) private address chosen for Q
Q_ke public key chosen for Q
Q_kd private key chosen for Q
Q_q question
Q_a

switching-center
gateway
user station

Fig. 2: Logical operation of the SBNS

B recognizes that b is one of its addresses and deciphers the message with the private key B_kd corresponding to b:
B_kd(B_ke(Q_p,Q_ke,Q_q)) = Q_p,Q_ke,Q_q.
B or a user at user station B, depending on the question, generates an answer Q_a.
B enciphers Q_a with Q_ke and sends Q_p,Q_ke (Q_a) to its gateway GB.
The gateway GB of B sends the received message to the switching-center.
The switching-center deciphers the address Q_p of A and splits it into the address ga of the gateway GA of A and Q_n, a pseudonym of A. The switching-center uses ga to send the message to the gateway GA of A.
The gateway GA of A broadcasts the received message.
A recognizes its private address Q_p and deciphers the answer with the corresponding private key Q_kd.

If it seems appropriate, using its idle time, B may have generated a random number R_n and computed a private address R_p = ke(gb,R_n). B also may have generated a public key R_ke and a corresponding private key R_kd.
B may send Q_p,Q_ke(R_p,R_ke,Q_a) to A instead of Q_p,Q_ke(Q_a).
This offers two advantages:

1) There is only one message format.
2) A may use the untraceable return address R_p,R_ke for the next communication with B, which makes traffic analysis even more difficult: There is no hint, that R_p has anything in common with b.

3.4 Performance, Reliability and Costs of local two-way broadcast networks

It is shown in [16] how all broad-band services of the German field trial "BIGFON" (Broad-Band Integrated-Services Fiber-Optic Local Network) can be offered to a group of 350 users using a 2 Mbit/s [1] optical fiber. If no broad-band services are offered, the bandwidth of the optical fiber is no longer the limit to the size of a user group. Then the reliability of the loop decreasing with every additional user or the performance of the gateway [8] is the limiting factor. If the SBNS is used for broad-band transmission, the encryption and decryption with public key cryptosystems cannot be provided using todays technology. If cryptography is necessary, A and B must use a private key cryptosystem (e. g. DES = Data Encryption Standard of the National Bureau of Standards [4 p. 9]), which can be applied to higher data rates. A and B must exchange the private key using the protocol described above before broad-band communication. The other resulting necessary changes of the above example are straightforward.

Essentially the same technique of exchanging a few bits of control information before broadband transmission may be used to ask the gateways and switching-centers to establish a broadband channel between two anonymous user stations. The allocated channel will be released after the session. By establishment of a fixed channel user observability may increase but network performance may increase as well [25] and user stations may become cheaper [16]: they only have to monitor a common channel which in this case need not be able to transmit broadband services and one or at most a few broadband channels.

A simple cost model with German prices suggests, that user groups of 10 to 700 users are economically feasible [16]. Economically feasible means, that the expected costs of the SBNS are less or equal than those of a star-shaped switched network. This surprising result stems from the fact, that a loop-shaped connection of user stations is usually much shorter than a star-shaped connection. Because the cost to bury cables is normally three times as high as the cost of broad-band cables, amplifiers etc. [28 p. 152] and the cost to bury cables is proportional to the length of the connection of the user stations, a loop-shaped connection may be cheaper even if its bandwidth must be higher to offer service comparable to that of a star-shaped connection.

4. DISTRIBUTED BILLING

Because most services offered by an ISDN aren't free of charge, there must be the possibility of billing users or user stations.
The classical form of billing in a switched network is as follows:

1) The switching-center (representing the

network operator) monitors the usage of network resources by user stations. Users are billed after certain time intervalls (e. g. monthly).

2) Added value (e. g. information or special service) providers know their clients and bill them directly or
the switching center is authorized to bill users for added values, too.
In the latter case, the switching center may hide the identity of clients from added value providers, but then the switching center can and must monitor the used added value services, too. This solution, which hinders added value providers to become "little brothers" by monitoring client behavior, enables the switching center to become "big brother". For further information see [13, 2, 5, 7, 14, 17].

Thus the classical form of billing is inappropriate in a SBNS.
Two solutions of the billing problem with complementary advantages and drawbacks are known.

4.1 Anonymous numbered account approach

The first solution is an advancement of a numbered account. (For in depth information on numbered accounts, please ask a Swiss bank, you may have multiple choices here at Zurich.)
To open an anonymous numbered account, you (or another person you trust) visit a company C (e. g. bank, network operator) which offers that service at the SBNS. You choose a company at which you are not personally known. The company C tells you an account-number an, you tell the company a public key an_ke generated by your user station, the corresponding private key an_kd will be the password for your anonymous numbered account. (If the used public key cryptosystem hasn't the property ke(kd(M)) = M, don't worry. In this case you tell the company a private key an_kd generated by your user station, the corresponding public key an_ke will be the password for your anonymous numbered account.)
You deposit an amount of your choice and receive a voucher.

If you want to use a service offered by the SBNS, which isn't free of charge, you have to use the protocol of chapter 3.3 with the following extensions:
Your user station generates an electronic cheque
F_ec = an,an_kd(time,sequence number,amount)
and transmits
b,B_ke(Q_p,Q_ke,Q_q),ke(c,c_ke(F_ec)).
c is an address of the company C, c_ke the corresponding public key, the other abbreviations are defined in chapter 3.3.
The switching-center deciphers the cheque with its private key kd.
The switching-center sends c,c_ke(F_ec) to C.
C deciphers the message with c_kd, looks up the key an_ke corresponding to an and uses an_ke to decipher
an_kd(time,sequence number,amount).
C checks the sequence number and time and determines min, the minimum of amount and the value v still available at the numbered account. C subtracts min from the numbered account: v := v-min.
C transfers ke(min,c_ke(F_ec)) to the switching-center which may now act like in the classical form of billing: the switching-center monitors the cost, abrupts the service when the costs exceed min and transfers min-costs to C when the service is finished.

C adds min-costs to the numbered account:
v := v+min-costs.

The advantages and drawbacks of the anonymous numbered account approach are obvious:

+ Anonymous numbered accounts and thus bills cannot be correlated to user stations.
+ Neither party can cheat:
  The user receives vouchers when depositing money.
  The company operating the anonymous numbered account gets cheques, which only the user could generate by use of its private key.
  For an in depth discussion on electronic funds transfers see [18].
- Depositing money may be troublesome (e. g. which company, at which he isn't personally known, should Ronald Reagan choose?).
- There may be a lot of extra message traffic for billing, if the company operating the anonymous numbered account isn't identical with the network operator.

4.2 Safeguarded counters at user stations

The second solution to the billing problem is an advancement of electricity billing.

All user stations are equipped with a safeguarded counter. Safeguarded means that the counter cannot be manipulated by the user. Every operation on the counter requires an inverse operation on another station's counter by means of a bill.
The counter adds the charges for the used services and subtracts the charges for the delivered services. The switching-center also has a counter to register the charges for the services of the SBNS. The switching-center regularly (e. g. monthly) reads the counters of the user stations and bills the users. If there are no pending bills, the sum of all counters is zero, which offers a possibility to check the integrity of the counters.
Implementation issues of the counters are mentioned in [11, 16, 21]. [16] presents algorithms to distribute counter values between instances in the network such that inconsistencies of counters in the presence of faults or fraud are limited, but user inobservability is maintained.

The necessary extensions of the protocol of chapter 3.3 are sketched below:
A user at user station A wants ...
B generates its answer Q_a and a bill Q_b. Generating Q_b, B subtracts the amount of Q_b from its counter.
B enciphers its answer and its bill with with Q_ke and sends Q_p,Q_ke(Q_a,Q_b) to its gateway GB.
The gateway GB ...
A recognizes its private address Q_p and deciphers the answer with the corresponding private key Q_kd. A adds the amount of Q_b to its counter. If the user of A doesn't agree with the received bill, he must negotiate with B about a difference-bill, because he cannot change the counter of his user station without changing the counter of another station inversely by means of a bill.

If transmission of messages by the SBNS is charged, the switching center appends bills to messages as well.
Disputes between users can be resolved, if digital signatures are used appropriately: B has to sign its bill and to store A's request for a certain time.

The drawbacks and advantages of the safeguarded counter approach are obvious:
- Regularly read values of safeguarded counters are correlated to user stations. If enough charged transactions take place between successive reads of the safeguarded counter, this is acceptable.
- If the user can cheat the safeguarded counter of its user station, the user may cheat all other users. This will be detected, but the cheater can not be localized.
+ Depositing money isn't necessary.
+ There's no extra message traffic for billing. Only the message length increases a bit.

5. FAULT TOLERANCE AND PROTECTION AGAINST FRAUD

In a loop-shaped two-way broadcast network, the sender destroys its message. For the purpose of fault tolerance, he may compare the received message with the message he sent. If there are any faults, he may retransmit the message.
In the switched ISDN the usual techniques to achieve fault tolerance may be used.
If the sender wishes to get back messages, which could not be transmitted to the recipient, he must attach a private address to each message, because the untraceable return address enciphered within the message can only be deciphered by the recipient.

Measures to prevent fraud depend on the solution of the billing problem.
If the anonymous numbered account approach is adopted, only keys must be kept secret.
If safeguarded counters at user stations are employed, there must be some provision to enforce registration of user stations. In [16] the transfer of secret information into a user station at its registration is proposed. This secret information is used in all communications by employing a secret key cryptosystem (e. g. DES) which uses the transfered secret information as secret key. User stations must erase the secret information when physically damaged. Implementations of this property are discussed in [11].

6. AVOIDANCE OF PATTERNS IN TIME

In the preceding chapters a network structure was described, which to some extent avoids and to the other tries to hide patterns in space of the message traffic:

* There's no cable which connects only one user station with the rest of the network.
* There's no bijection addresses -- user stations.

Another problem remains to be solved: patterns in time of the message traffic must be avoided.

E. g., if only one user of a user group is doing night-work, it's not hard to guess who, after returning from work, regularly transfers a message at 3 o'clock a. m. to receive an electronic evening newspaper.

The following measures help to avoid patterns in time of the message traffic:

M1 Whenever possible, the user station chooses the time of a message transfer at random in a time interval given by user expectations or cheap night rates.
In the world of the above example our user, before he leaves for his night-shift, instructs his user station to request the evening newspaper between 9 o'clock p. m. and 2 o'clock a. m..
Besides decreasing user observability M1 reduces costs by distributing traffic load.

M2 User stations or gateways may generate dummy traffic when there's not enough message traffic.

7. COMPARISIONS

The only other solution of the traffic analysis problem I know is the solution of Chaum [3]. He gives a protocol which hides sender and receiver of a message in a switched network from each other. The protocol guarantees hiding, if at least one of the switching-centers which the message passes performs the protocol correctly and hides the information it gains.

Chaum's and my protocols make massive use of public key cryptosystems. Because different functions in the network are the security-hardcore of the two protocols, the decrease in user observability of the two protocols is difficult to compare.

Both protocols depend to a certain extent on the security of the public key cryptosystem they use. Because both protocols use a lot of keys only once and decrease user observability even if some of the ciphers are broken, both don't need ultra-security of the public key cryptosystem they use.

Chaum's protocol depends on the fact that at least one switching-center doesn't cheat. This may be as hard to believe as that all switching-centers don't cheat, if all switching-centers are operated by the same company (e. g. PTT's in Europe). If one switching-center of the company cheats, all may cheat. Chaum's protocol operates in batch mode. Otherwise the dummy traffic required to hide patterns in time of the message traffic would become prohibitive. Thus Chaum's proposal isn't appropriate for the real time traffic in an ISDN. Another problem of Chaum's protocol is that the complexity of untraceable return address generation grows quadratic with the number of switching-centers which execute his protocol with the passing message.

My proposal depends on the assumption, that the loop-shaped two-way broadcast network is not tapped directly before and behind a user station. Tapping directly before and behind a user station can be made difficult by the cable run.

For an electronic mail system Chaum's protocol and my proposal can be combined.

I hope, together we have found or will find political and technical solutions to the problems of 1984.

ACKNOWLEDGEMENTS

Suggestions, criticism and encouragement of Prof. Winfried Görke, Birgit Pfitzmann and Prof. Detlef Schmid are gratefully acknowledged.

REFERENCES

[1] Clemens Baack, Gerhard Elze, Gerd Grosskopf, Godehard Walf:
Digital and Analog Optical Broad-Band Transmission;
Proceedings of the IEEE, Vol. 71, Nu. 2, February 1983, pp. 198-208

[2] Hans Peter Bull:
Datenschutz und neue Medien;
Datenschutz und Datensicherung, 3/1982, pp. 147-152

[3] David L. Chaum:
Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms;
Communications ACM Vol. 24, Nu. 2, February 1981, pp. 84-88

[4] Data Security in Computer Networks;
IEEE computer, Vol. 16, Number 2, February 1983

[5] Neue Medien und Datenschutz; Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)
Beschluß der 7. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Berlin am 11. Dezember 1980
Datenschutz und Datensicherung, 3/1981, pp. 200-201

[6] Dorothy Elizabeth Robling Denning:
Cryptography and Data Security;
Addison-Wesley Publishing Company, Reading, Mass., 1982

[7] Hansjürgen Garstka:
Anforderungen des Datenschutzes an Gesetze auf dem Gebiet der neuen Medien;
Datenschutz und Datensicherung, 3/1982, pp. 153-156

[8] A. Grant, D. Hutchison, W. D. Shepherd:
A Gateway for Linking Local Area Networks and X.25 Networks;
SIGCOMM '83 Symposium Communications Architectures & Protocols, University of Texas at Austin, March 1983, Computer Communication Review, Vol. 13, Nu. 2, pp. 234-239

[9] Richard desJardins:
ISO Open Systems Interconnection Standardization Status Report;
SIGCOMM '83 Symposium Communications Architectures & Protocols, University of Texas at Austin, March 1983, Computer Communication Review, Vol. 13, Nu. 2, pp. 4-5

[10] Hiroyuki Kasai, Kenji Ohue, Takashi Hoshino, Shigeru Tsuyuki:
800 Mbit/s Digital Transmission System Over Coaxial Cable;
IEEE Transactions on Communications, Vol. COM-31, No. 2, February 1983, pp. 302-306

[11] Walter Kuntz:
Schutz der Software und Hardware von Microrechnern gegen Mißbrauch;
Handbuch der modernen Datenverarbeitung (HMD), Forkel-Verlag, Heft 109, Januar 1983, 20. Jahrgang, ISSN 0723-5208, pp. 129-133

[12] Ernst L. Leiss:
Principles of Data Security;
Plenum Press, New York, London, 1982

[13] George Orwell:
1984;
A Novel by George Orwell, With a special Preface by Walter Cronkite, and an Afterword by Erich Fromm, Revised and Updated Bibliography; A Signet Classic, New American Library, Times Mirror, New York, 1983

[14] Ulrich v. Petersdorff:
Das Kompetenzproblem und die datenschutzrechtliche Verantwortlichkeit bei Bildschirmtext;
Datenschutz und Datensicherung, 2/1981, pp. 83-86

[15] Andreas Pfitzmann:
Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien;
GI '83 13. Jahrestagung der Gesellschaft für Informatik 3. bis 7. Oktober 1983, Universität Hamburg, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, pp. 411-418

[16] Andreas Pfitzmann:
Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes;
Fakultät für Informatik, Universität Karlsruhe, Internal Report 18/83, December 1983

[17] Günter Reiner:
Datenschutz und Bildschirmtext;
Datenschutz und Datensicherung, 2/1981, pp. 87-90

[18] Karl Rihaczek:
OSIS - Open Shops for Information Services;
DuD Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Friedr. Vieweg & Sohn, Braunschweig, Heft 2, April 1983, pp. 116-125

[19] R. L. Rivest, A. Shamir, L. Adleman:
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems;
Communications ACM Vol. 21, No. 2, February 1978, pp. 120-126

[20] J. H. Saltzer, K. T. Pogran, D. D. Clark:
Why a Ring?
Computer Networks, The International Journal of Distributed Informatique, North-Holland, Vol. 7, Nu. 4, August 1983, pp. 223-231

[21] Softwareschutz in Einchip-Mikrocomputern; Sicherungs-Bit im EPROM;
Markt&Technik Nr. 42 vom 21. Oktober 1983, pp. 60-62

[22] Adi Shamir:
On the Generation of Cryptographically Strong Pseudorandom Sequences;
acm Transactions on Computer Systems, Vol. 1, Nu. 1, February 1983, pp. 38-44

[23] Andrew S. Tanenbaum:
Computer Networks;
Prentice-Hall, Englewood Cliffs, N. J., 1981

[24] Andrew S. Tanenbaum:
Network Protocols;
acm computing surveys Vol. 13, Nu. 4, December 1981, pp. 453-489

[25] Fouada A. Tobagi:
Multiaccess Protocols in Packet Communication Systems;
IEEE Transactions on Communications, Vol. COM-28, No. 4, April 1980, pp. 468-488

[26] Donald W. Davies:
tutorial: The Security of Data in Networks;
IEEE Catalog No. EH0183-4, 1981

[27] Cay Weitzman:
Distributed Micro/Minicomputer Systems;
Prentice Hall, Englewood Cliffs, N. J., 1980;

[28] Wolfgang Kaiser:
Interaktive Breitbandkommunikation;
Nutzungsformen und Technik von Systemen mit Rückkanälen;
Telecommunications, Veröffentlichungen des Münchner Kreis, Band 8, Springer-Verlag Berlin Heidelberg New York, 1982