Research on anonymous communication in German(y) 1983-1990

Andreas Pfitzmann
TU Dresden, Fakultät Informatik, D-01062 Dresden
Phone +49 351 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Site to download the original papers and reports:
http://dud.inf.tu-dresden.de/sireneLit.shtml
Aims of my talk

• Make historic knowledge (pre WWW, originally written mostly in German) available

• Give a tutorial on basic techniques mostly forgotten, but – in my opinion – terribly useful and terribly needed in designing today’s and tomorrow’s (IP v6) communication systems

• Learn from 20+ years history to re-focus PET research and development
Switched/broadcast network (1983 - 1985)

Switched WAN (possibly including MIXes) connecting broadcast LANs (RING-net, DC-net)

- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks
Switched/broadcast network (1983 - 1985)

Switched WAN
(possibly including MIXes)
connecting
broadcast LANs
(RING-net, DC-net)

- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks
Switched/broadcast network (1983 - 1985)

Switched WAN (possibly including MIXes) connecting broadcast LANs (RING-net, DC-net)

- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks
Switched/broadcast network (1983 - 1985)

- Switched WAN (possibly including MIXes) for services tolerating longer delays connecting broadcast LANs (RING-net, DC-net)

- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks
RING-net (1983-1985)
Digital signal regeneration:
The analogue characteristics of bits are independent of their true sender.
Digital signal regeneration:

The analogue characteristics of bits are independent of their true sender.

alternatives: 123... $n+1$
RING-net (1983-1985)

Digital signal regeneration:
The analogue characteristics of bits are independent of their true sender.

The idea of physical unobservability and digital signal regeneration can be adapted to other topologies, i.e. tree-shaped CATV networks;
RING-net (1983-1985)

Digital signal regeneration:
The analogue characteristics of bits are independent of their true sender.

The idea of physical unobservability and digital signal regeneration can be adapted to other topologies, i.e. tree-shaped CATV networks;

It reappears in another context in Crowds
Braided RING (1985-1987)

Two RINGs operating if no faults

Reconfiguration of the outer RING if a station fails

Reconfiguration of the inner RING if an outer line fails

Reconfiguration of the outer RING if an outer line fails
Addressing in broadcast networks (1985)

### Addressing

- **explicit addresses:** routing
- **implicit addresses:** attribute recognizable by the station of the recipient

<table>
<thead>
<tr>
<th></th>
<th>addr dist</th>
<th>public address</th>
<th>private address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>invisible</strong></td>
<td></td>
<td>very costly, but necessary to establish contact</td>
<td>costly</td>
</tr>
<tr>
<td><strong>visible</strong></td>
<td></td>
<td>should not be used</td>
<td>change after use</td>
</tr>
</tbody>
</table>

- **invisible public address</===> asymmetric cryptosystem**
- **invisible private address</===> symmetric cryptosystem**
Anonymity of the sender

If stations are connected by keys the value of which is completely unknown to the attacker, tapping all lines does not give him any information about the sender.

D. Chaum 1985 for finite fields
A. Pfitzmann 1990 for abelian groups
Anonymity of the sender

If stations are connected by keys the value of which is completely unknown to the attacker, tapping all lines does not give him any information about the sender.

D. Chaum 1985 for finite fields
A. Pfitzmann 1990 for abelian groups
Anonymity of the recipient: Fail-stop key generation (1989-91)

- DC-net provides recipient anonymity only against a passive attacker – an active attacker might manipulate the consistency of the broadcast.
- Fail-stop key generation (use the locally received result of round \( r \) as one input to calculate the keys for all rounds to come) guarantees consistency unconditionally, which yields unconditional recipient anonymity even against computationally unrestricted active attackers.


Superposed receiving (1988-1990)

Whoever knows the sum of \( n \) characters and \( n-1 \) of these \( n \) characters, can calculate the \( n \)-th character.

**pairwise superposed receiving** (reservation scheme: \( n=2 \))

Two stations send simultaneously.
Each subtracts their character from the sum to receive the character sent by the other station.

\[ \Rightarrow \text{Duplex channel in the bandwidth of a simplex channel} \]

**global superposed receiving** (direct transmission: \( n \geq 2 \))

Result of a collision is stored, so that if \( n \) messages collide, only \( n-1 \) of them have to be sent again.

Collision resolution algorithm using the mean of messages:

\( \leq 2^T - 1 \) stations \hspace{1cm} \text{addition mod } 2^L \]

\[
\begin{array}{cc}
  T \\
  0 \ldots 0 \hspace{2cm} \text{message} \hspace{2cm} T-1 \\
  \hline
  & 0 \ldots 0 & 1 \\
\end{array}
\]

Overflow area for addition of messages

Overflow area for addition of counters

Counter
Pairwise superposed receiving (1988-1990)

Without superposed receiving

\[ (X+Y)-X = Y \]

With pairwise superposed receiving

\[ (X+Y)-Y = X \]

Global superposed receiving (1988-1990)

Collision resolution algorithm with mean calculation and superposed receiving

Time division partitioning of the tree and appropriately chosen dynamic key graphs:

In the first time partition (potentially) global (e.g. international) traffic takes place: all messages travel to the root and are broadcast world-wide. Keys for this time partition can (and should be) shared with other user stations all over the world.

In the $n+1^{st}$ time partition, all messages travel only to the $n^{th}$ sons of the root (representing e.g. continentals, states, districts, ...). Keys for these time partitions are only shared between user stations which are sons of the same $n^{th}$ son of the root.

A. Pfitzmann: How to implement ISDNs without user observability - Some remarks; Interne Bericht 14/85, Univ. Karlsruhe, Fak. Informatik, p. 67
Fault tolerance: sender-partitioned DC-net (1990)

Write and read access to DC-net

Read access to DC-net
Possible propagation of errors by station 3
Fault tolerance: sender-partitioned DC-net (1990)

Write and read access to DC-net
Read access to DC-net
Possible propagation of errors by station 3
by station 5
Enhancements of MIXes (1985-1990)

Symmetric crypto for first and last MIX

Channels: reduce delay (and storage),
but must start and end at the same time

--> time-slice channels

Constant rate dummy traffic end-to-end having 3 advantages:
1. real-time behavior of batch MIXes
2. unobservable sending and receiving of messages
3. when combined with cascade,
   • MIXes may substitute traffic for users to hide their
     presence/absence or failures of their machines or
     counter active attacks
   • linkability of some messages does not change the
     anonymity more than absolutely unavoidable
Requirements: ISDN services using the ISDN transmission system

- 2 independent 64-kbit/s duplex channels using 144-kbit/s subscriber lines
- nearly no delay on established channels
- establishment of channels within 3 seconds
- no additional load to the long-distance network

network structure

A’s local exchange

B’s local exchange

64+64+16 = 144 kbit/s duplex
Time-Slice Channels (1989)

Station A  MIXes (A)  l. ex.(A)  l. ex.(B)  MIXes (B)  Station B

$t_t$

- tsc-s setup: $x$
- tsc-r setup: $x$

- tsc-s setup: $y$
- tsc-r setup: $y$

$y$

- tcs-s
- tcs-r

Call request: $k$, sA und sB

- tsc-s setup: PRG(sB,1)
- tsc-r setup: PRG(sA,1)

- tsc-s setup: PRG(sA,1)
- tsc-r setup: PRG(sB,1)
**Time-Slice Channels (1989)**

Station A  MIXes (A)  l. ex.(A)  l. ex.(B)  MIXes (B)  Station B

\[ t_0 \]
- tsc-s setup: \( x \)
- tsc-r setup: \( x \)

\[ t_1 \]
- tcs-s
- tcs-r \( x \)
- tsc-s setup: \( \text{PRG}(sB,1) \)
- tsc-r setup: \( \text{PRG}(sA,1) \)

Call request: \( k, sA \) und \( sB \)

Broadcast

\[ t_0 \]
- tsc-s setup: \( y \)
- tsc-r setup: \( y \)
Time-Slice Channels (cont.)

\[ t_2 \]
- \( \text{tsc-s setup: PRG}(sB,2) \)
- \( \text{tsc-r setup: PRG}(sA,2) \)

\[ t_3 \]
- \( \text{PRG}(sA,2) \)
- \( k(\text{data}) \)
Delayed acceptance of call

Station A  MIXes (A)  l. ex.(A)  l. ex.(B)  MIXes (B)  Station B

t₀

- tsc-s setup: x
- tsc-r setup: x

from P  PRG(sQ,0)  tcs-r

t₁

- tsc-s setup: PRG(sB,1)
- tsc-r setup: PRG(sA,1)

- call request: k, sA und sB

- tsc-s setup: PRG(sP,0)
- tsc-r setup: PRG(sQ,0)

- from P  PRG(sQ,0)  tcs-r
- to P  tcs-s

- tsc-s setup: PRG(sP,1)
- tsc-r setup: PRG(sQ,1)
Delayed acceptance of call (cont.)

$t_2$
- tsc-s setup: $\text{PRG}(sB,2)$
- tsc-r setup: $\text{PRG}(sA,2)$

$t_{t-1}$
- tsc-s setup: $\text{PRG}(sB,t-1)$
- tsc-r setup: $\text{PRG}(sA,t-1)$

$t_t$
- PRG$(sA,t-1)$
- PRG$(sB,t-1)$
- k(call accept, data)
Advantages of Real-Time MIXes

- recipient anonymity without untraceable return addresses with long validity (good for fault tolerance)
- cascade: pipelining -> even distribution of processing of traffic without any stochastic assumptions
- together: avoiding any need of long term storage of (hashes of) messages


“Proof” of MIX cascade (1990)

Maximum anonymity means (possibilistic setting):
• all other senders or recipients of the messages of a particular time interval
  or
• all MIXes
have to cooperate to trace a message against the wish of its sender or
recipient.

Assuming that each message is mixed by each MIX only once, to achieve
maximum anonymity, all these messages have to pass each MIX
simultaneously and therefore all the MIXes in the same order (→ MIX
cascade). (Remark: In a probabilistic setting, this would hold as well.)

Proof (ind.): Assume not all these messages pass each MIX simultaneously,
then there exist a MIX i and two messages $m_1$ and $m_2$ which do not pass
MIX i simultaneously. If all other MIXes except i cooperate, they can trace $m_1$
and $m_2$ before and after MIX i. If all other senders and recipients than those
of $m_1$ and $m_2$ cooperate, this means that both $m_1$ and $m_2$ are completely
traceable, if no other senders or recipients cooperate, it means that the
anonymity set of both $m_1$ and $m_2$ is decreased.

Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbares
Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990. ISBN 3-540-52327-8, p. 69
“Proof” of MIX cascade (cont.)

MIX 1

\[ \text{m1} \rightarrow \text{m2} \]

MIX \( i \)

\[ \text{m1} \rightarrow \text{m2} \]

MIX \( n \)
“Proof” of MIX cascade (cont.)
“Proof” of MIX cascade (cont.)

Proof diagram:

- MIX 1
- MIX i
- MIX n

- m1
- m2
Fault-tolerance within the MIX-net (1985-1990)

2 alternate paths through disjunct MIXes

MIX$_i$ or MIX$_i''$ can replace MIX$_i$
Fault-tolerance within the MIX-net (cont.)

Single MIXes can be skipped

coordination protocol
## At which layer? (1985-1990)

<table>
<thead>
<tr>
<th>OSI layers</th>
<th>Broadcast</th>
<th>MIX-net</th>
<th>DC-net</th>
<th>RING-net</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 application</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 presentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 session</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 transport</td>
<td>implicit addressing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 network</td>
<td>broadcast</td>
<td>batch and change encoding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 data link</td>
<td>channel selection</td>
<td>superpose messages and keys</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 physical</td>
<td></td>
<td></td>
<td>digital signal regeneration</td>
<td></td>
</tr>
<tr>
<td>0 medium</td>
<td></td>
<td></td>
<td></td>
<td>ring</td>
</tr>
</tbody>
</table>

- Yellow: has to preserve anonymity against the communication partner
- Green: end-to-end encryption
- Orange: has to preserve anonymity
- Brown: can be built without regard to anonymity
Lessons I learned

1. strong (but completely hypothetical in 1985) **attacker models** got reality in the meantime, cf. interfaces for law enforcement in all communication networks; nevertheless, the research community mainly addresses weaker attacker models in the last 10 years than David Chaum and my group did 1983-1990

2. **Quality of Service** (QoS): delay very low + throughput high, otherwise anonymity and unobservability will never get a service to the masses, but the PET research community considers mainly P2P, i.e. ignores QoS, when the Internet community finally starts to get QoS aware (e.g. IP v6)

3. anonymity and unobservability work well with **isochronous traffic** (common in channel switched networks)

4. 2. and 3. suggest that the PET community will finally rediscover **isochronous (dummy) traffic** in future

5. the **interface** between anonymous communication and applications has to have **as less assumptions as possible**, cf. dummy traffic, static networks ...