



telesoft
TECHNOLOGIES

Intelligent Probing for Intelligence and LI Applications

Presented by

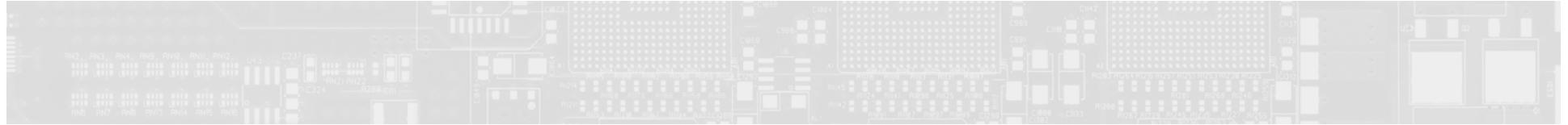
Keith Driver - Telesoft Technologies

February 2007 v1.0



Topics

- What is Intelligent Probing?
 - How is it achieved?
 - What can be achieved?
 - How relevant is this to 3G networks?



What is Intelligent Probing?



Intelligent Probing is:

- Selective Acquisition of data, based on network signalling and bearer properties
 - E.g. DTMF tones, original called number, type of call
 - Not just called/calling party numbers
- Handling of incomplete network data
- Real time network data Analysis
 - CIC mapping derivations
 - Multiple Subscriber Identity/Location correlations

Goals

- To provide precise event selection capability
 - To provide independent access to network data across network types
 - (GSM/CDMA/3GPP/PSTN/Sattelite)
 - To provide a single central interface for handover of the information
 - To operate in imperfect environments

Intelligent Probing



Probing both signalling and communication content

- Signalling, examining ALL signalling parameters, not just called/calling party numbers
 - Original Called Number
 - Redirecting Number
 - Calling Party Category ... etc
 - Prefix/Suffix/wildcard matching
 - Number normalisation
 - Communications Content
 - DTMF digit extraction
 - Activity (Energy) detection in timeslots
 - Classification of content (Fax/Modem/Voice)

Complex event selection

- ➊ Call selection based on complex criteria
 - Calls from A to B
 - Calls from A to B redirected to C
 - Calls only from B
 - All Fax calls
 - All Modem calls from A to B
 - All events on a declared circuit
 - Events where timeslot energy > -20dBm
 - SMS from A to C when B is located with A



Independent Access

- ➊ Intelligent Probes are mostly passive (non-intrusive), and therefore independent
- ➋ Intelligent probes are purpose designed
- ➌ Able to Acquire data from different networks/interfaces
- ➍ Provide Standardised Handover Interfaces ETSI / CALEA / TIIT etc

Implementation of Intelligent Probes

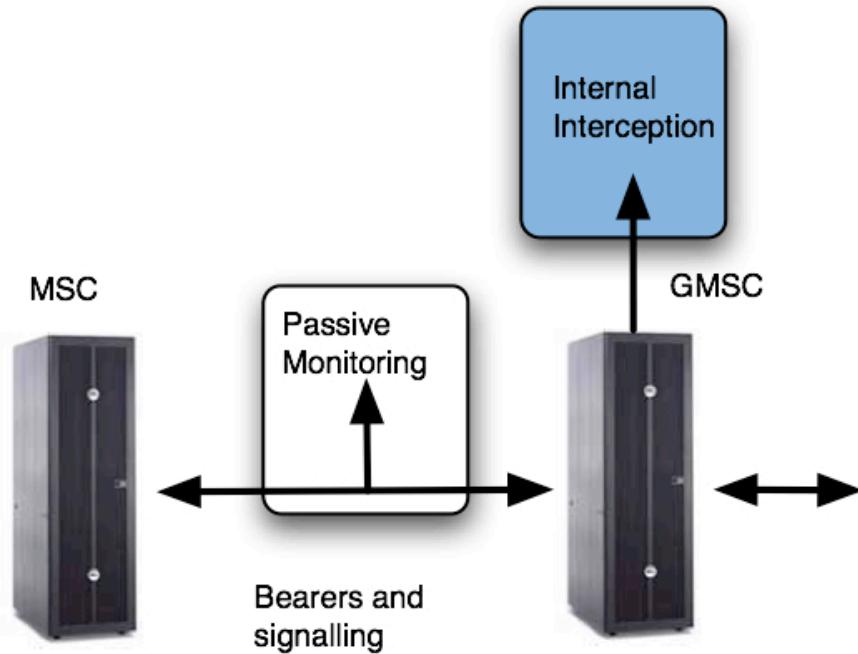


Acquiring network data occurs in two ways

- Forwarding from existing infrastructure
 - ‘Internal Interception’
 - Manufacturer specific implementation
 - Limited functionality, hard to extend and slow to do
 - Non core function to network node
 - Generally focused on minimum LI requirements
- Passive monitoring of interconnects
 - Generic access to network data
 - Rich functionality, easy and fast to extend
 - Specialised equipment
 - Wide range of capability
 - Less ‘visible’

Internal Interception Function

- ➊ Acquisition from
 - Network nodes
 - Passive tapping
- ➋ Each has advantages





Internal vs Off Switch

Internal

– Pros

- No extra equipment necessary
- Handover interface implemented within the equipment
- Access to internal data structures can make it more efficient

– Cons

- Each manufacturer implements the interface differently
- Provisioning of target data is not uniform
- Manufacturers often charge for the feature
- The switch is forced to perform a non-core task and takes resources from core tasks
- The switch must be tasked with the LI warrants
- An upgrade in switch s/w can ‘break’ the LI feeds
- On switch solutions can introduce detectable artefacts



Internal vs ‘Off Switch’



Off Switch

– Pros

- LI function will not affect the network performance or customer experience.
- Independent of network equipment and vendors. A single interface presented.
- Defined interfaces for remote tasking.
- More intelligence can be placed in the probe, greatly benefiting the LEA.
- The same equipment can be used for Intelligence intercept as for LI.

– Cons

- More equipment must be deployed and managed.

Architecture

- Truly intelligent probes can only be offered through passive access
 - Passive monitoring also confers
 - A single handover interface for all LI/Intelligence data
 - Single provisioning point
 - Electronic provisioning
 - Physically Centralized target holding - more secure

Operation in Imperfect environments

- ➊ Lawful Intercept usually allows for full access to signalling and bearers
- ➋ Intelligence gathering is more opportunistic.
- ➌ Intelligent probes derive data from incomplete intercept data
 - Only one path (Tx or Rx) of the signalling and or bearers may be available
 - Data may be of poor quality (high error rate)
 - Only a proportion of bearers may be accessible
 - Some signalling may be load shared across links that are not accessible
- ➍ Intelligent Probes have specific algorithms for this



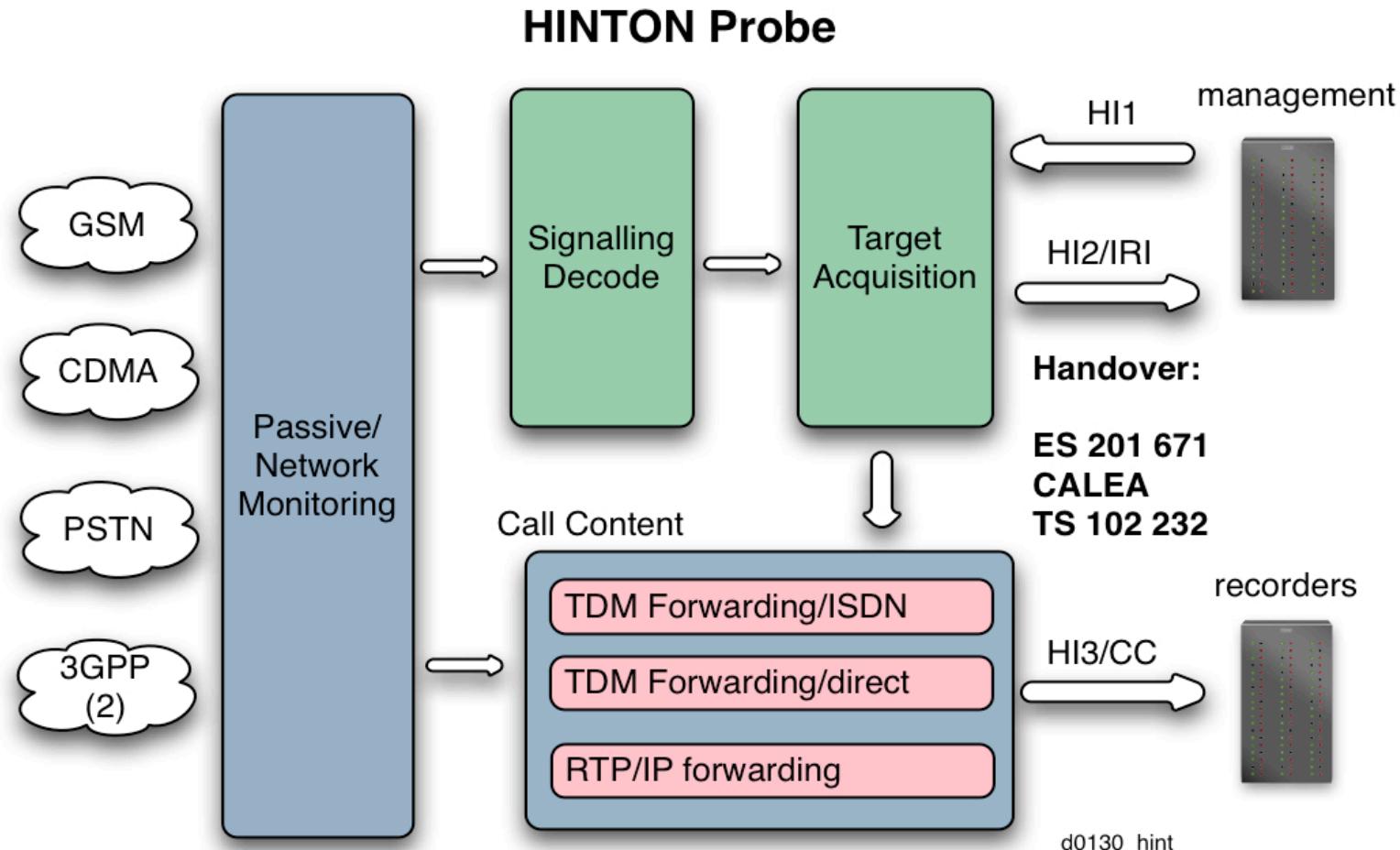
How is it Achieved?



Passive Access

- ➊ Passive Access through tapping of electrical and optical bearers
- ➋ Remote and distributed probe deployment
- ➌ Backhaul to centralised processing

Accumulated handover



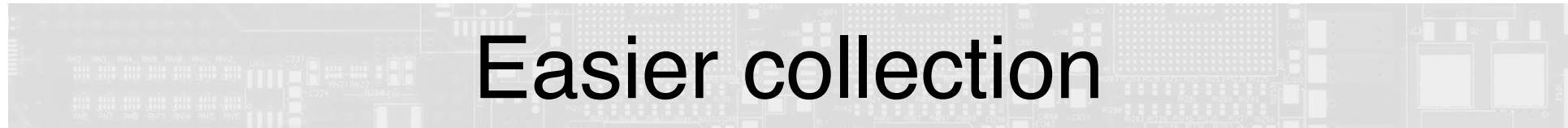


Accumulated Handover

- ➊ Network signalling and content is probed from the observed network
- ➋ Events are relayed to the central processing server over transfer network
- ➌ The server makes decisions on recording and meta data creation (CDR's / IRI etc)
- ➍ The probes are instructed to stream the call content to a destination recorder.
- ➎ All decisions are made centrally



What can be Achieved?



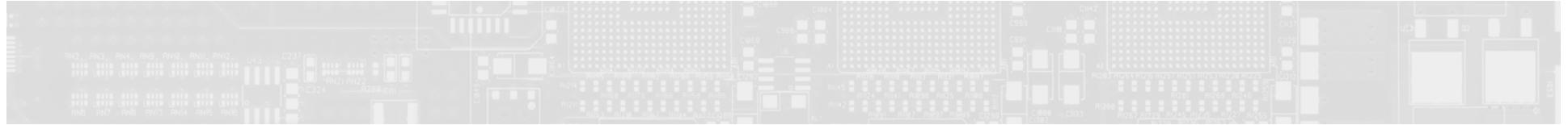
Easier collection

- ➊ Large scale network monitoring from a single interface
 - Disparate technologies, interfaces, locations
- ➋ Clandestine/opportunistic access
- ➌ Access with greater security
- ➍ Passive solution means no compromise to network integrity



Easier processing

- ➊ Lower volume of acquired data for analyst processing, through better selection
- ➋ Automatic processing of data flows
 - e.g. (Fax-->demodulator->OCR->keyword recognition)
- ➌ Event triggers based on target proximity /accumulation/absence
- ➍ Event triggers based on communication content.



How Relevant is this to 3G networks?

Packet based Networks

- Networks are being converged/replaced with packet based transport
 - Telephony is still the primary service of such networks, and therefore must be acquired
 - Mandated Internal functions scavenge resource limiting capacity
 - Selection of the correct flows from packet networks is even more important

Access to packet transmission

- ➊ Passive access to packet transports is needed
 - WAN links with PoS, or the 3GPP IuXX interfaces with ATM/HDLC transports
 - SIGTRAN signalling transports
 - Packet accumulation and forwarding
 - LAN links with hardware support for Deep Packet inspection in real time
- ➋ But the analysis is identical

Legal considerations

- ➊ The Legal position for packet networks will be very complex. Unwarrented collection may be key to national security.
- ➋ Media Gateways may be located outside jurisdiction, but signalling will be inside
- ➌ Warrants for target installation in equipment not owned by the authority will not be possible



Intelligent Probing provides

- Precise targeting
- Reduced workload for analysts- reduced volumes
- More secure collection of data
- Independent and immediate access to data
- Sophisticated triggers (location / proximity)
- Network nodes are not required to perform non-core tasks



A better solution for Intelligence, and for Lawful Intercept



Further Information



<http://www.telesoft-technologies.com>

- HINTON product range
 - GSM/CDMA/PSTN/Sattelite probes
 - 3GPP Iu/Nb/Nc probes
 - OSS Probes
 - Lawful Intercept/Intelligence probes
 - Probes for revenue generating applications
 - Missed Call/Welcome Roamer/



Thank you for watching



telesoft
TECHNOLOGIES

www.telesoft-technologies.com

Telesoft Technologies Ltd
Observatory House
Blandford Dorset
DT11 9LQ UK

T. +44 (0)1258 480 880
F. +44 (0)1258 486 598
E. sales@telesoft-technologies.com

Telesoft Technologies Inc
Suite 601
4340 Georgetown Square
Atlanta GA 30338 USA

T. +1 770 454 6001
F. +1 770 452 0130
E. salesusa@telesoft-technologies.com