Boxed Out:
Blocking Cellular Interconnect Bypass Fraud at the Network Edge

Brad Reaves*, Ethan Shernan**, Adam Bates*, Henry Carter**, Patrick Traynor*

*Florida Institute for Cyber Security
University of Florida

**Georgia Institute of Technology

Presented By: Gohar Irfan

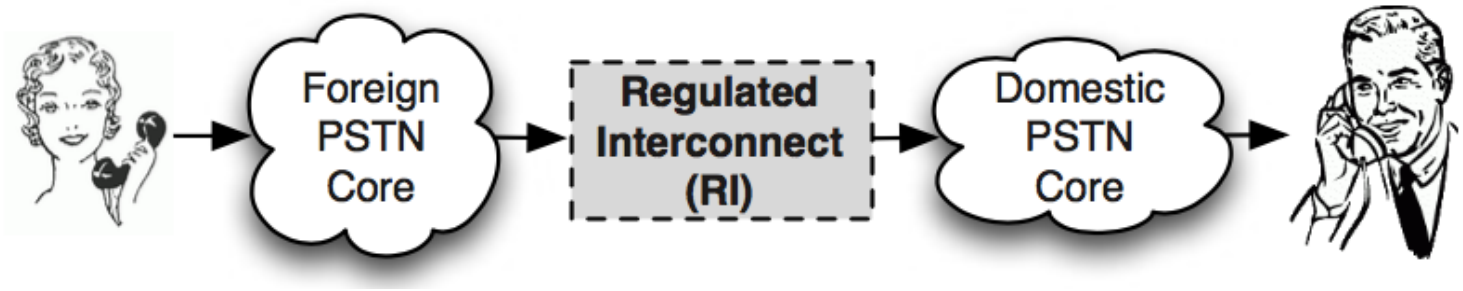
Are you happy with your long distance carrier?

There is a black market for long-distance and international call termination

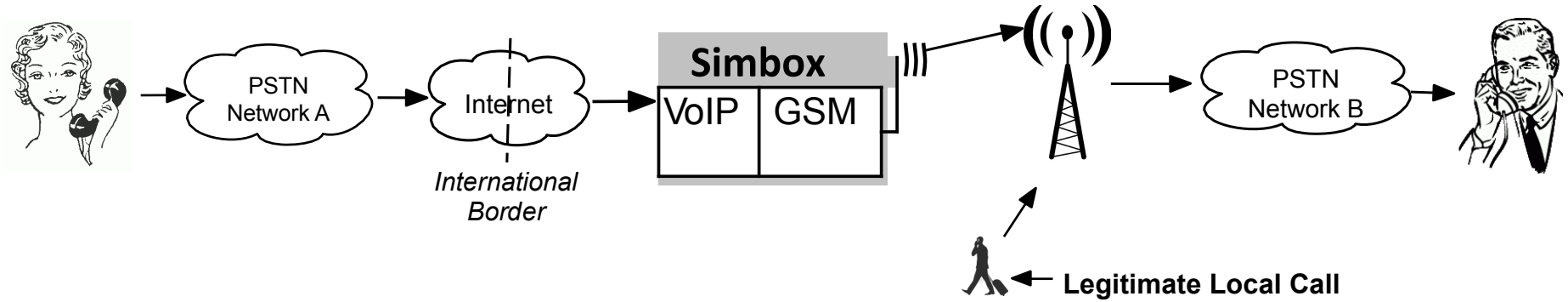
Some companies provide “gray routes” that deliver calls without paying required tariffs or using regulated interconnects between carriers

How do you connect to a carrier without them knowing?

Typical International Call



Enter: Simbox Fraud



The point of this setup is to deliver a call into carrier B without paying for a real interconnection with that carrier.

Carriers use the term “interconnect bypass fraud”
We’ll use the term **“simbox fraud”** for this talk

This is a real problem

Cellular networks are necessarily provisioned under an assumptions of average call volume/cell

The cellular network is *fundamentally* incapable of supporting the load of an illicit, unlicensed telecommunications provider

Not to mention:

- Call quality is terrible
- People near the simbox operation have trouble placing calls
- It costs carriers $2 Billion annually

Cellular Networks

- GSM (Global System for Mobile Communications)
  - 2G
  - 3G
  - 4G LTE

- SIM (Subscriber Identity Module)
- GSM Full Rate (GSM FR) for encoding

VoIP

- Voice over Internet Protocol
  - IP Only
  - IP-PSTN
- Carried over UDP
- Characteristics:
  - Packet loss
  - Jitter
  - Gaps are filled by silence (default)
  - PLC (Packet Loss Concealment Algorithms)

Simbox

- Connects VoIP calls to GSM network
- There is a strong legitimate market for these
  - Private Enterprise Telephone Networks
- Support hundreds of SIM cards and codecs
- “Sim Servers” − use “virtual SIM cards” for calls

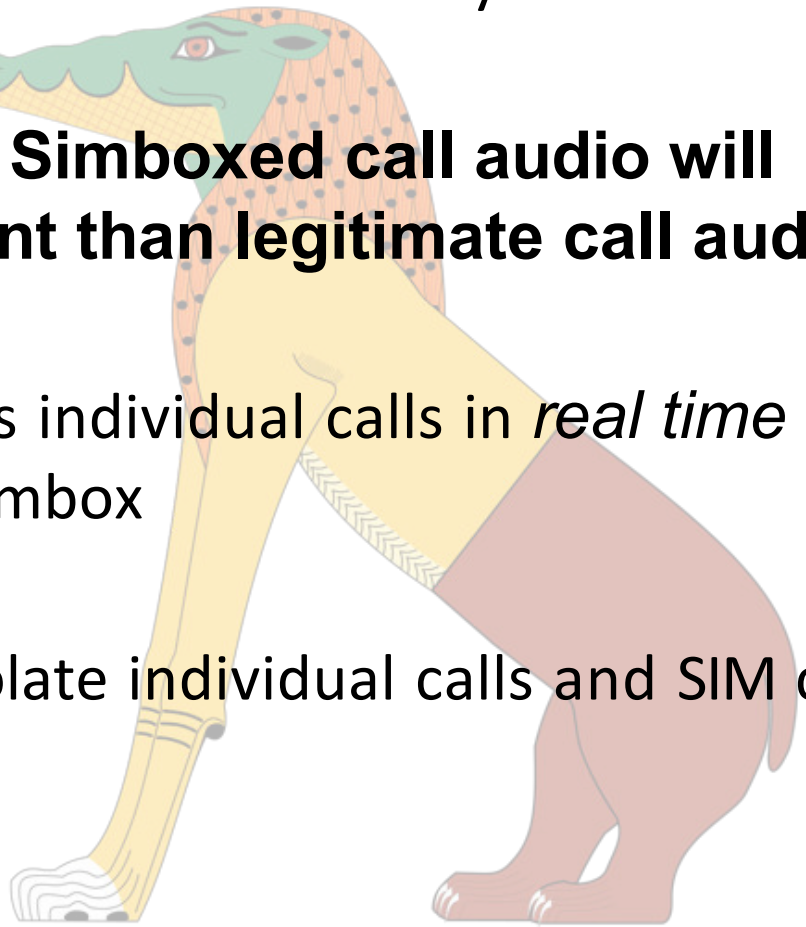
Ammit

- This work presents the Ammit system

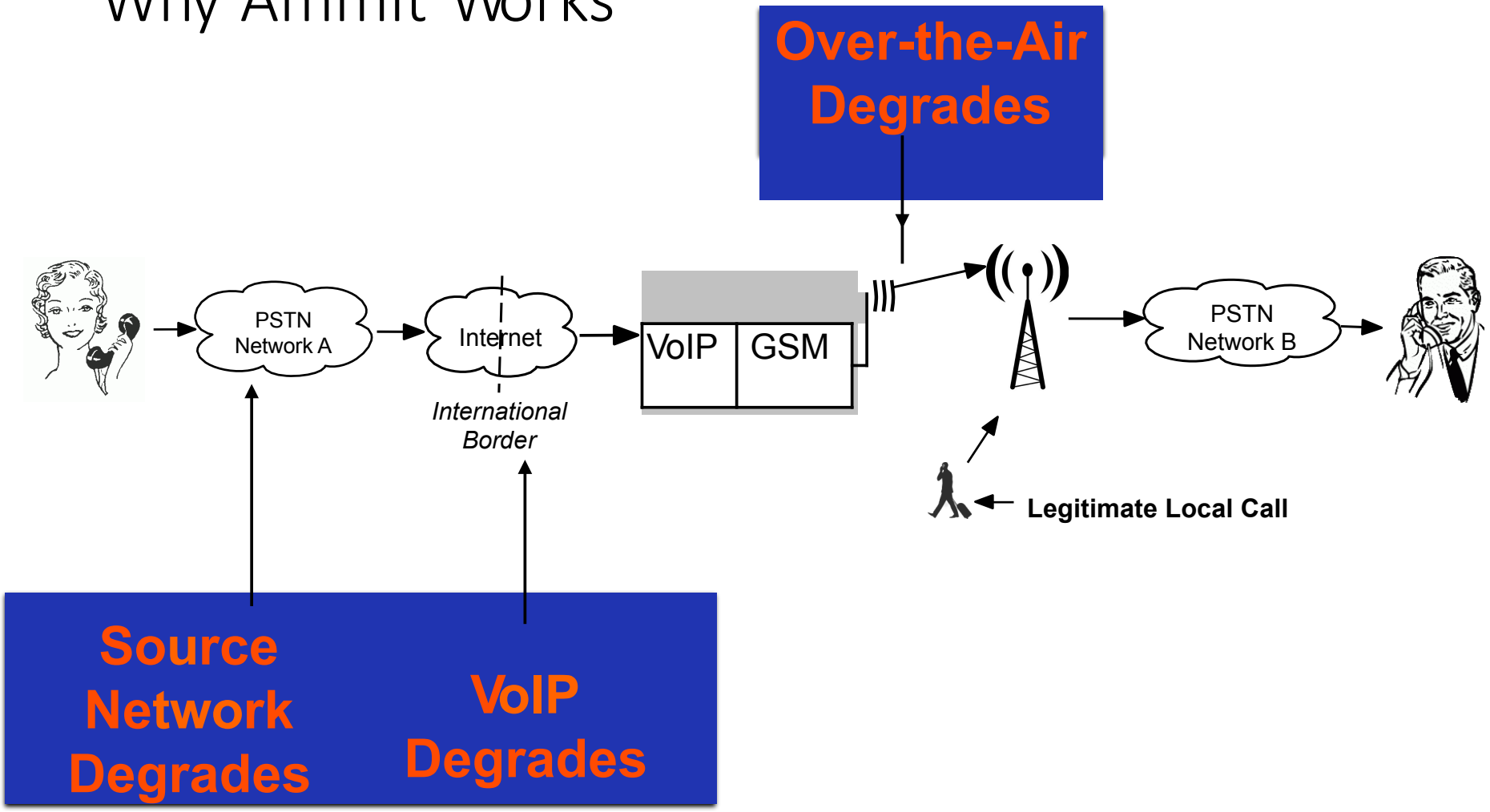
- **Key Insight: Simboxed call audio will sound different than legitimate call audio**

- Ammit detects individual calls in *real time* at the tower servicing the simbox

- Ammit can isolate individual calls and SIM cards after just 20 calls



Why Ammit Works



Dealing with Air Loss

Cellular voice sees typical loss rates of several percent

How are we supposed to tell legitimate losses from losses due to simboxing?

Have the tower keep track of lost frames and ignore them when analyzing the audio!

Audio degradations in VoIP

Because VoIP is entirely digital, audio only degrades from lost (or really late) packets

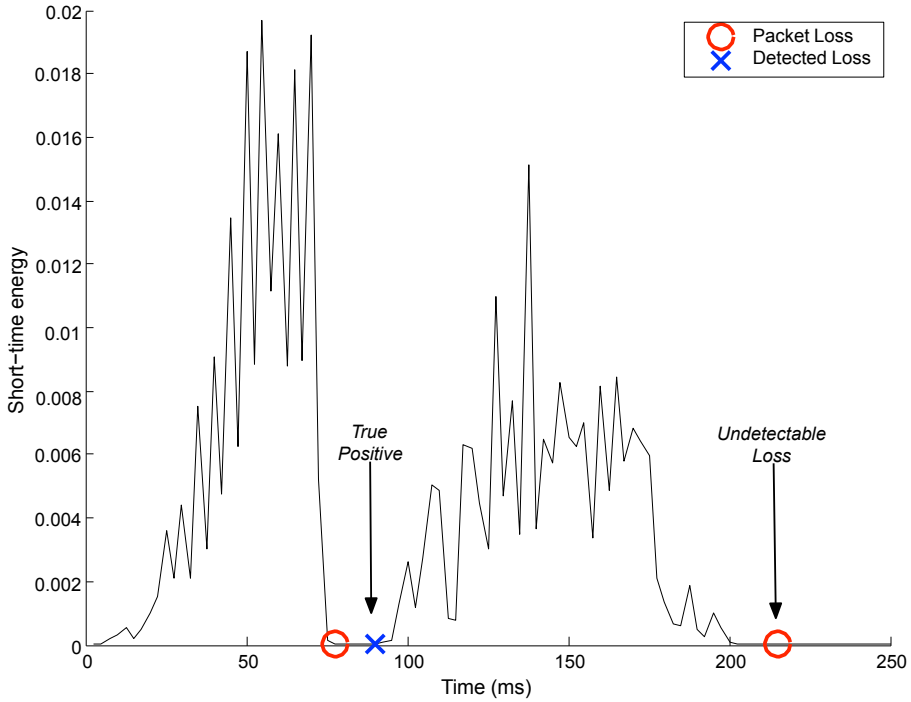
When losses occur, a VoIP client can either:

1. Insert silence

2. Try to conceal packet losses

Detecting Unconcealed Losses

We can compute the short-term energy of audio and look for sudden drops and rises again



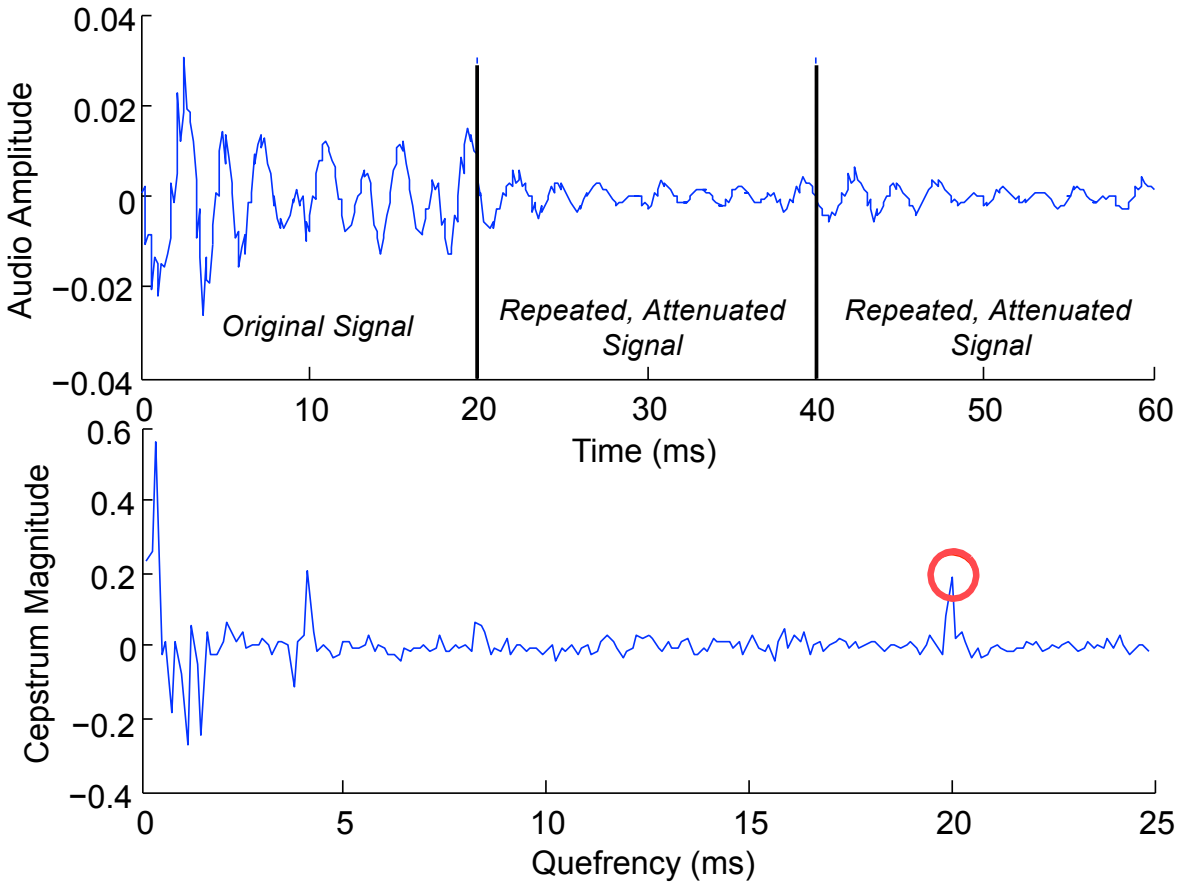
Detecting concealed losses

Authors looked at the GSM-FR packet loss concealment algorithm

GSM-FR conceals losses by repeating and attenuating the last good 20 millisecond frame.

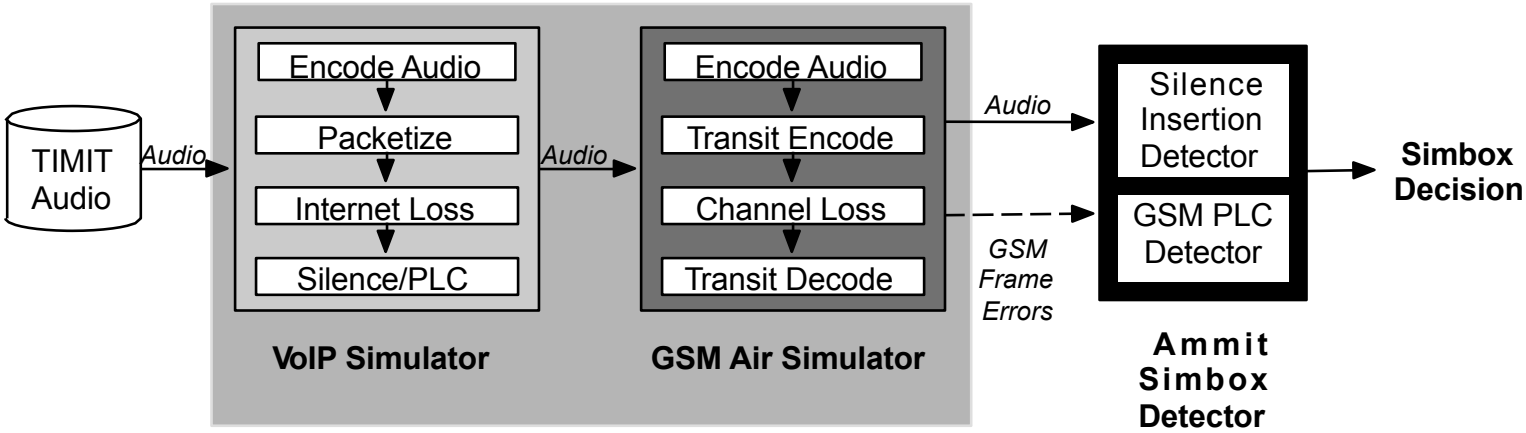
Cepstral analysis (used for echo detection) can detect this

GSM-FR Loss


0.04
0.02
0
−0.02
−0.04
Audio Amplitude
Original Signal
Repeated, Attenuated Signal
Repeated, Attenuated Signal
0
10
20
30
40
50
60
Time (ms)
0.6
0.4
0.2
0
−0.2
−0.4
Cepstrum Magnitude
0
5
10
15
20
25
Quefrency (ms)

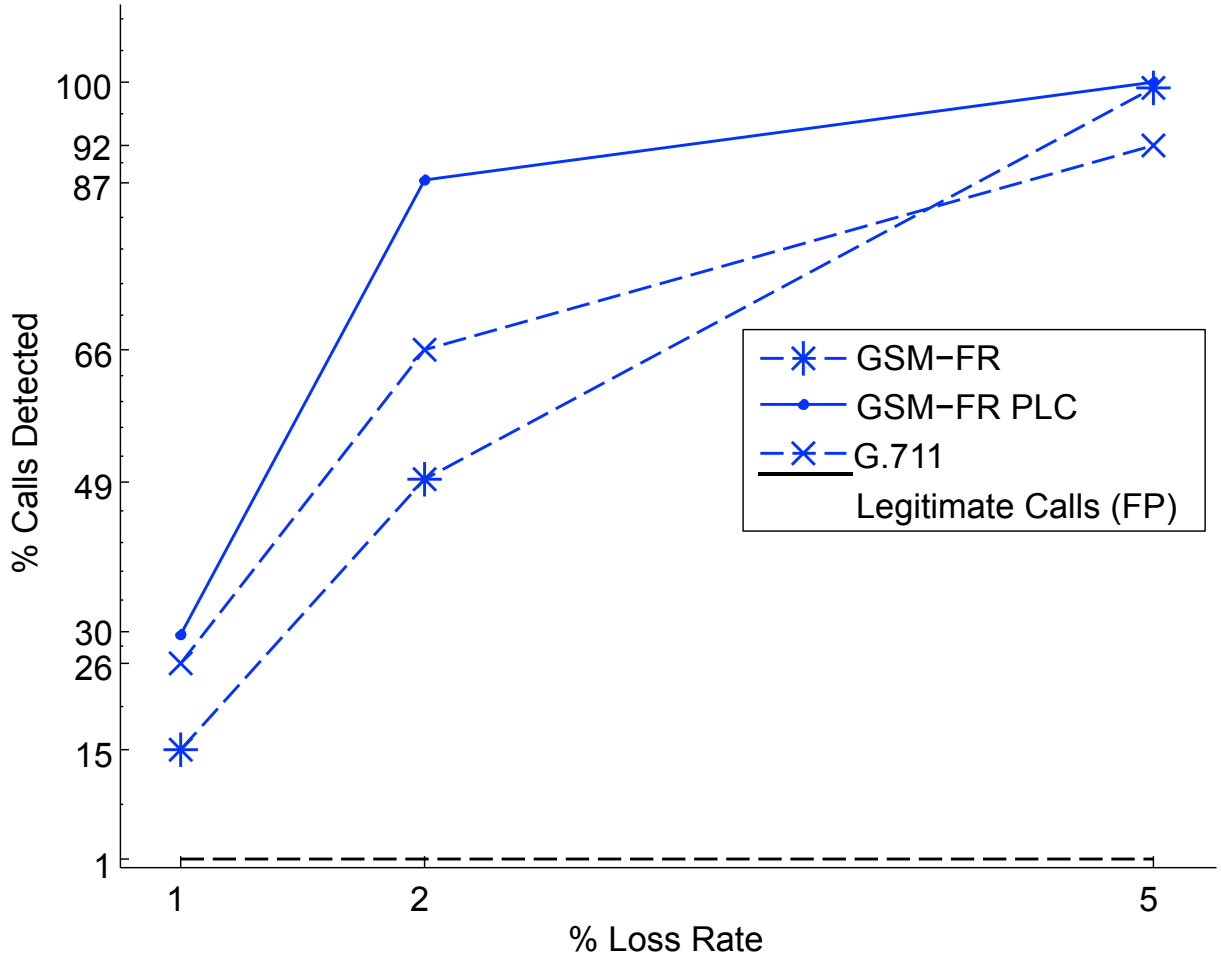
Simulation Setup

Tested Ammit on 462 individual simulated calls to systematically measure effect of loss rate and codec

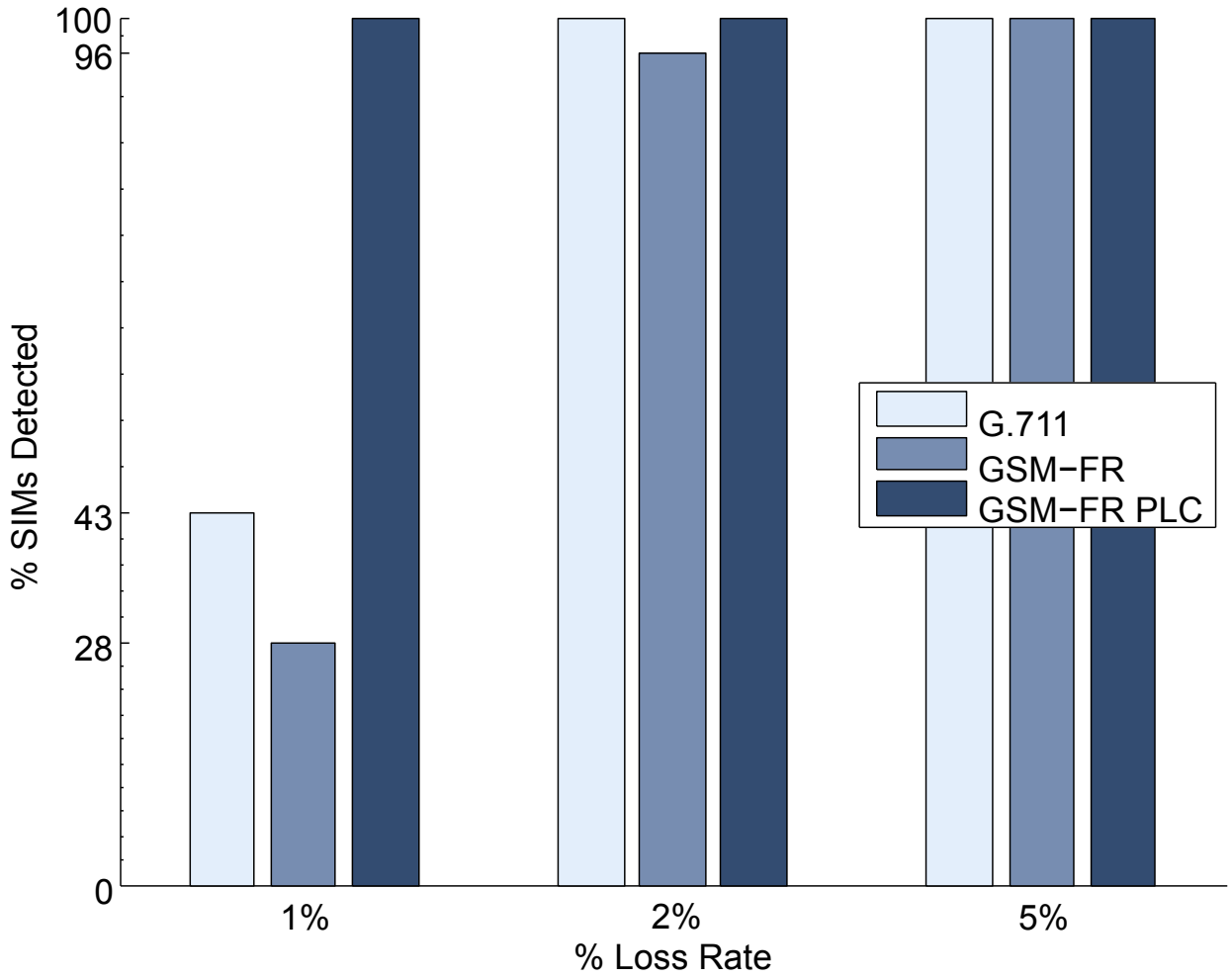


Simulated sets of 20 calls from 99 speakers to test effects of detecting multiple calls from a single SIM

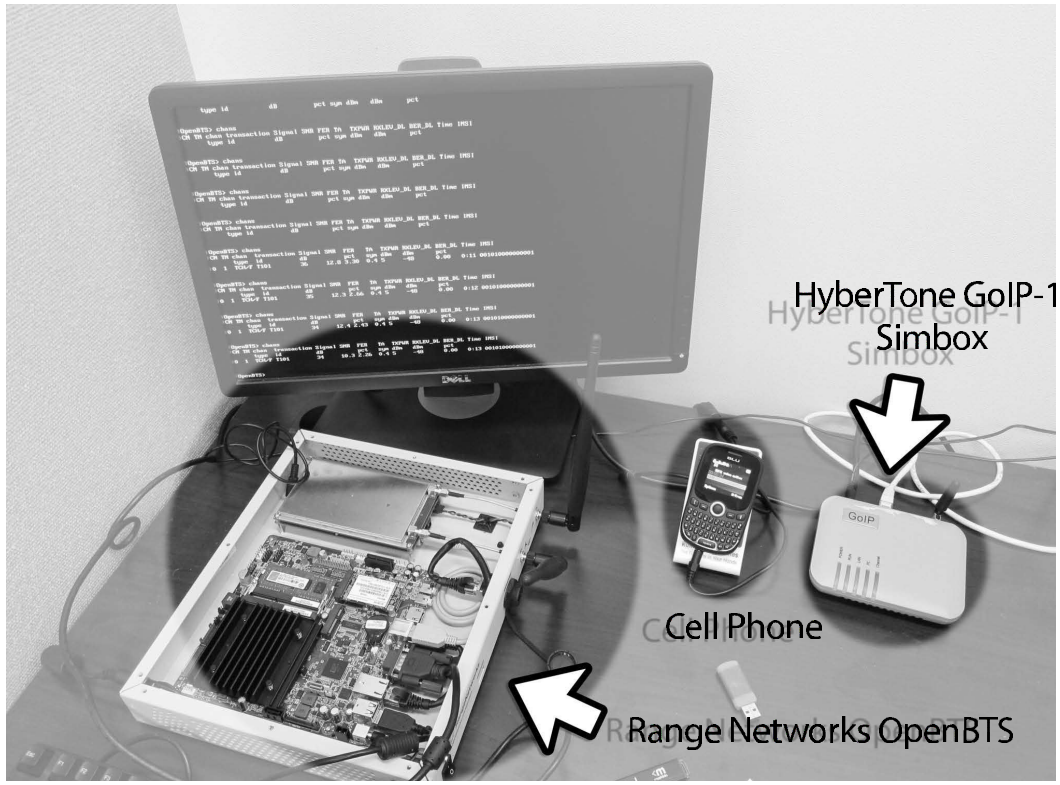
Results: Individual Simulated Calls



Results: Detecting Simulated SIMs



Results: Real Simbox Calls



- 100 simboxed and normal calls
- 87% of simboxed calls detected — no false positives

Security Assumptions

Ammit hardware and software no less accessible to attackers than network core (e.g. billing systems)

Ammit analyzes *all* call audio

(Our implementation could handle up to 150 simultaneous calls.)

Ammit reports single-call judgements to a central location (like the HLR)

Ammit is widely deployed (to prevent trivial evasion)

Potential evasions

Simboxers may try to evade Ammit, but it will be hard to do.

Here are some tricks they could try:

Redundantly transmit audio to avoid packet loss (expensive)

Try PLC's that Ammit doesn't know about (Most are known)

Transmit bad VoIP frames to the tower as damaged GSM frames (really hard and probably detectable)

Take-aways

The use of simboxes for interconnect bypass fraud represent a threat to the reliable function of cellular networks that billions rely on.

Ammit uses call audio to detect simbox calls in real time, stopping them at the source before they can be profitable

Discussion:

- Why is this approach good/bad?
- Can you think of ways to circumvent Ammit?
- Would this be practical to install in real telephone networks?
- What happens if you have an ideal loss-less VoIP connection?