SoK: Fraud in Telephony Networks

Merve Sahin, Aurélien Francillon

EURECOM
Sophia Antipolis

Partially in cooperation with:
Payas Gupta, Pindrop
Mustaque Ahamad, Georgia Tech

Telephony Fraud

- 1870s: Closed telephone network, trusted operators →
  2010s: Multiple parties involved, various
  technologies & services, IP convergence
- Performing fraud is easy and low risk
  - Easily monetized services
  - Massive volume of traffic
  - Remote attacks with little technical knowledge

Cost of Telephony Fraud

- Fraud loss estimated by operators was $38.1 billion in 2015[1]
  - 1.69% of total revenue

[1] CFCA Global Fraud Loss Survey, 2015

Cost of Telephony Fraud

- What about cost to society (financial, social, psychological)?
  - US Federal Trade Commission (FTC) receives an average of 400,000 complaints per month[1]
  - In France, 574,000 voice spam complaints received in 2016[2]

[1] National Do Not Call Registry, 2016

[2] 33700 Platform against Voice and SMS spam, 2016

Cost of Telephony Fraud

- Critical infrastructure that millions of users rely on
  - (e.g., Telephony DoS on emergency services*)

[*] Guri et al., “9-1-1 DDoS: Attacks, Analysis and Mitigation”, EuroS&P'17.

Cost of Telephony Fraud

- Telephony vulnerabilities also affect online security: e.g.,
  - Online account hijacks by social engineering telcos' customer representatives
  - Technical support scammers installing remote administration tool / malware *
  - Leakage of recorded telemarketing calls that include sensitive information (addresses, credit card numbers..)

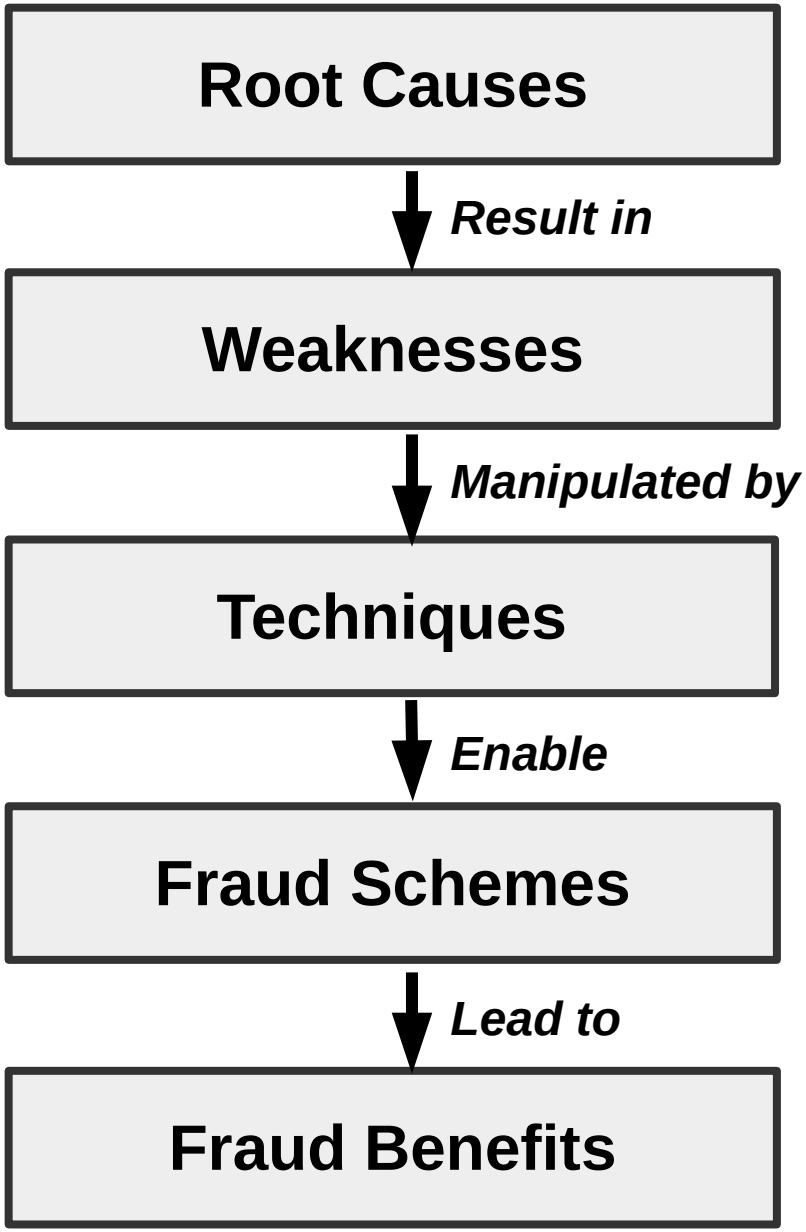
Motivation

- Telephony is considered as a trusted medium, but it is not always!
- **We need a better understanding of fraud to effectively fight it.**

Exploring the fraud ecosystem: Challenges

- Telephony fraud is a multi-dimensional problem
  - technology, environment, victim, techniques, impact...
- Fraudsters have various skills and motivations
  - Every actor has a different fraud experience
- Current fraud terminology can be confusing and misleading
  - Different terms for the same problem
  - Same term for different problems
- Public documentation is limited (e.g., restrictions from industry associations), sometimes incomplete (e.g., whitepapers)

Analyzing fraud in multiple layers



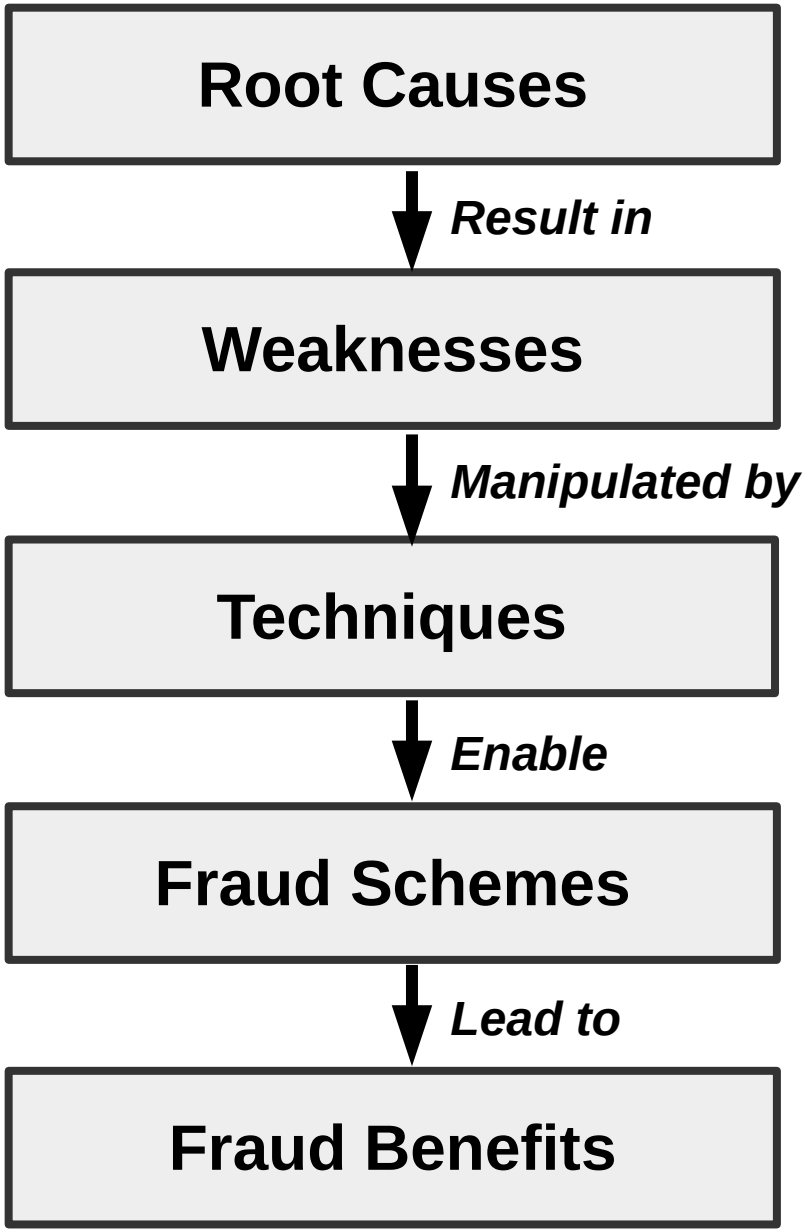
- A **fraud scheme** is a way to obtain an **illegitimate benefit** using a **technique**. Such techniques are possible because of **weaknesses** in the system, which are themselves due to **root causes**.

Example: Wangiri (Callback) Scam

Example: Wangiri (Callback) Scam

- Japanese word for “One (ring) and cut”

Example: Wangiri (Callback) Scam



Legacy/Insecure protocols, Interconnection of poorly understood technologies

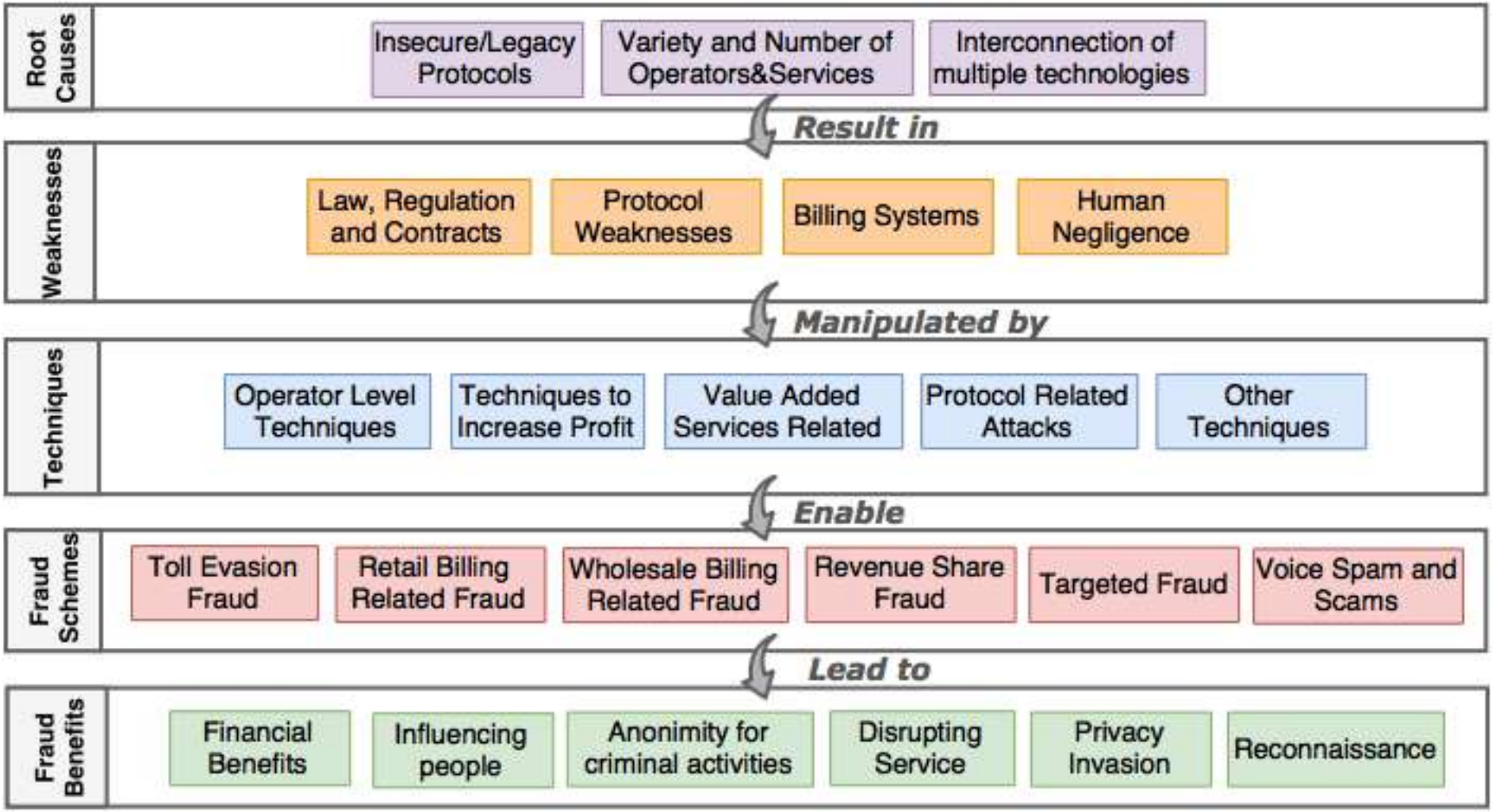
Lack of Caller ID authentication, Lack of security & fraud awareness

Caller ID spoofing, Auto-dialers, Social engineering

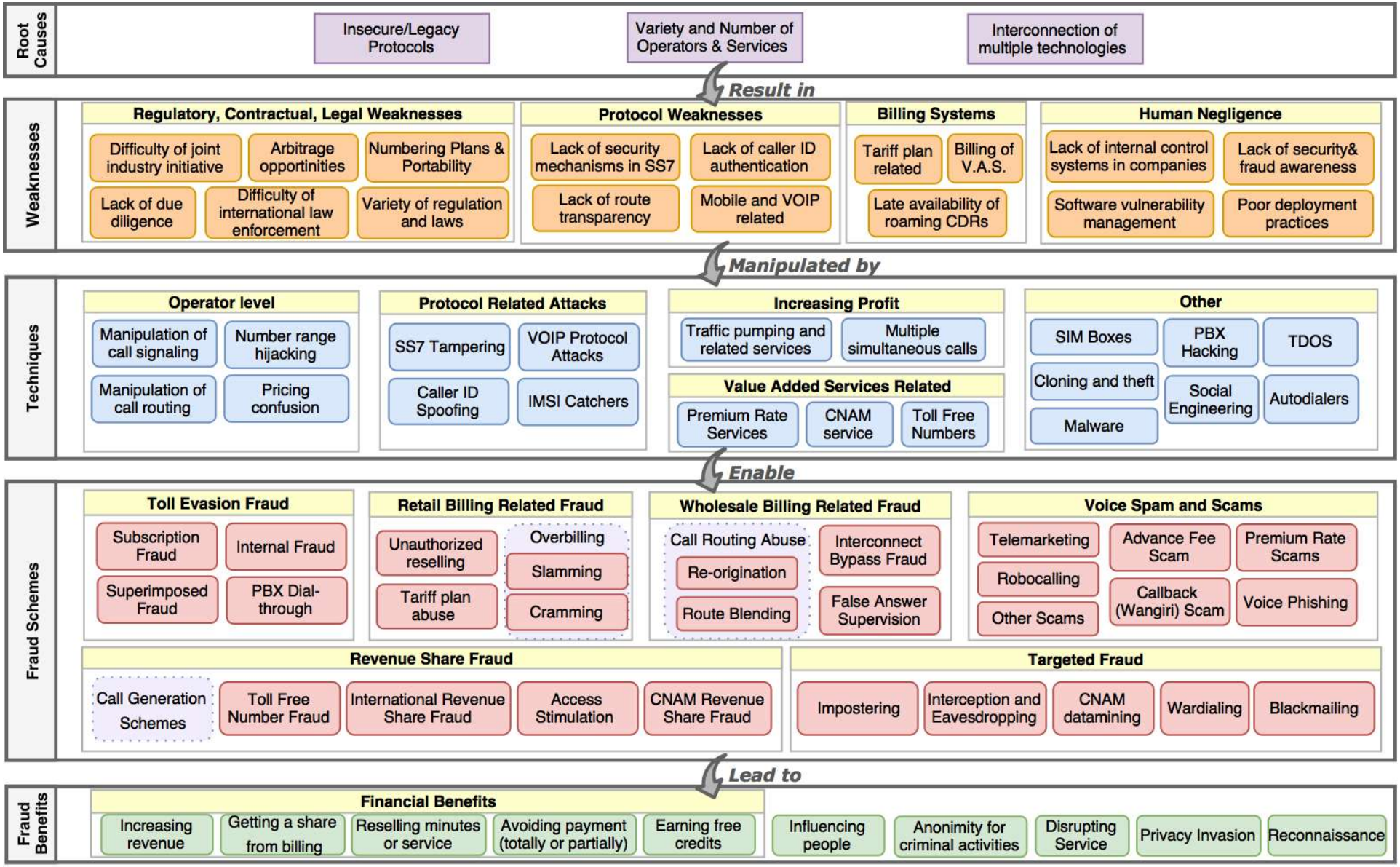
Callback (Wangiri) scam

Get a share from call revenue

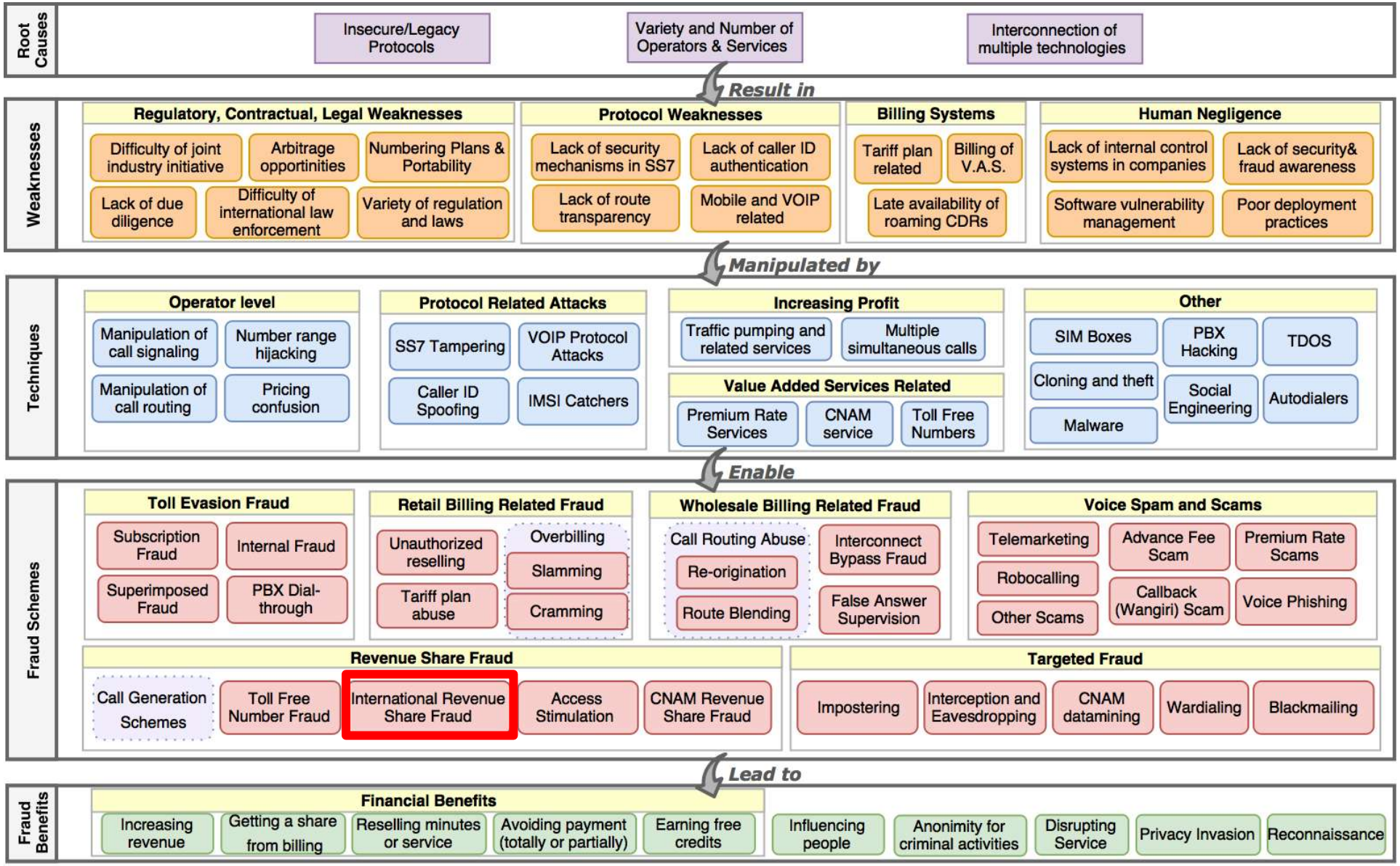
Our taxonomy



Our taxonomy



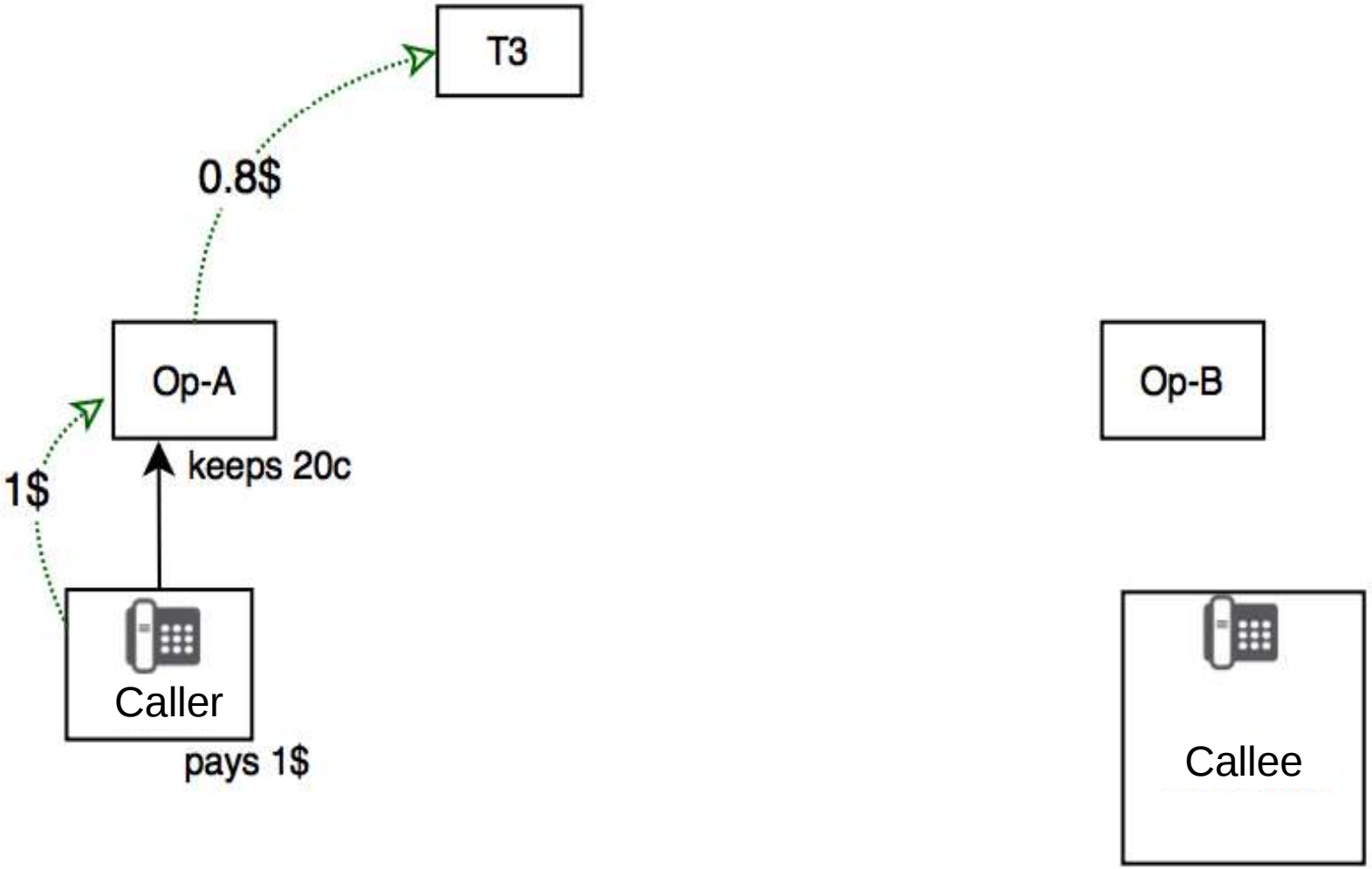
Example: International Revenue Share Fraud



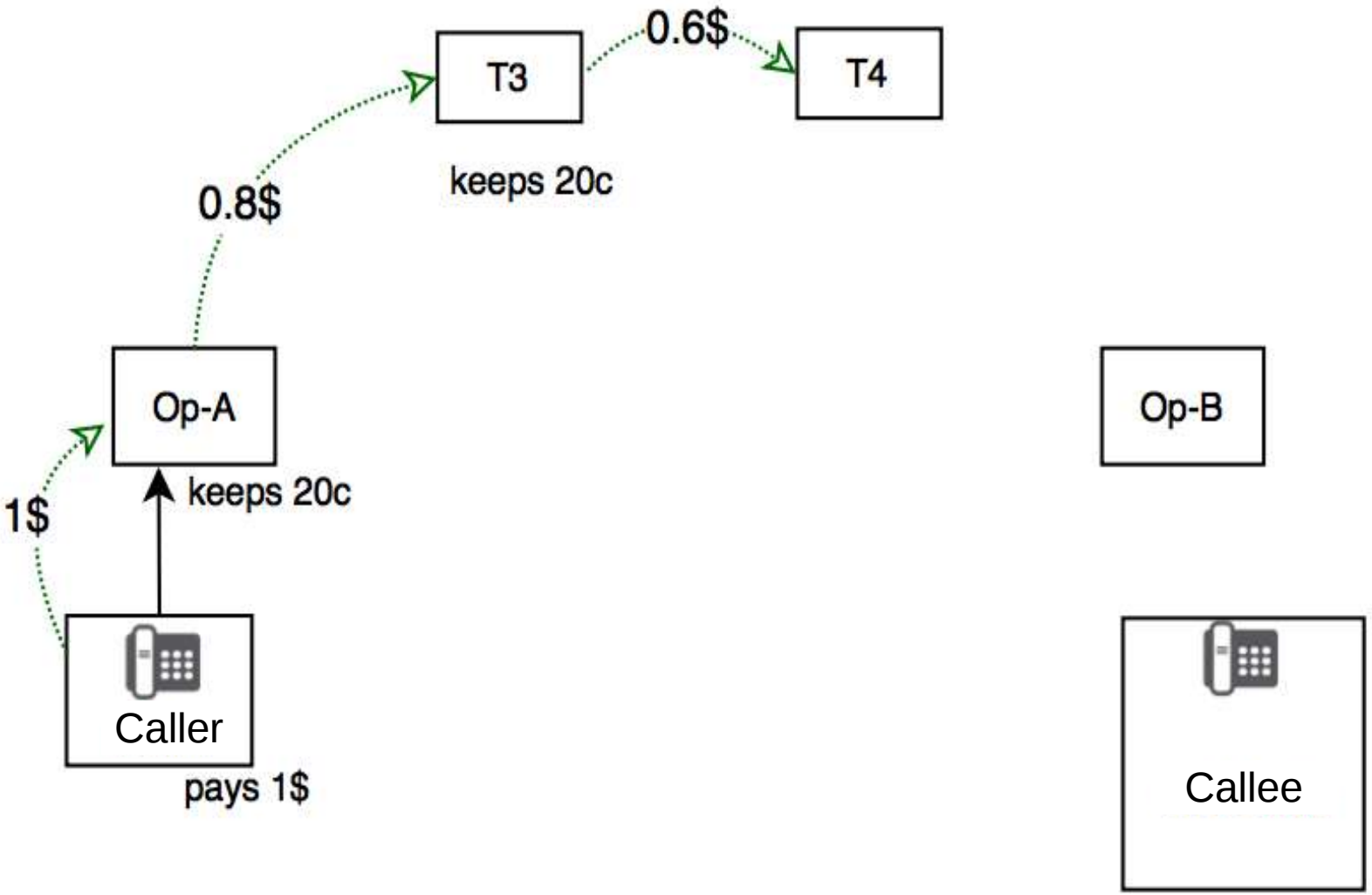
Regular International Call

Regular International Call

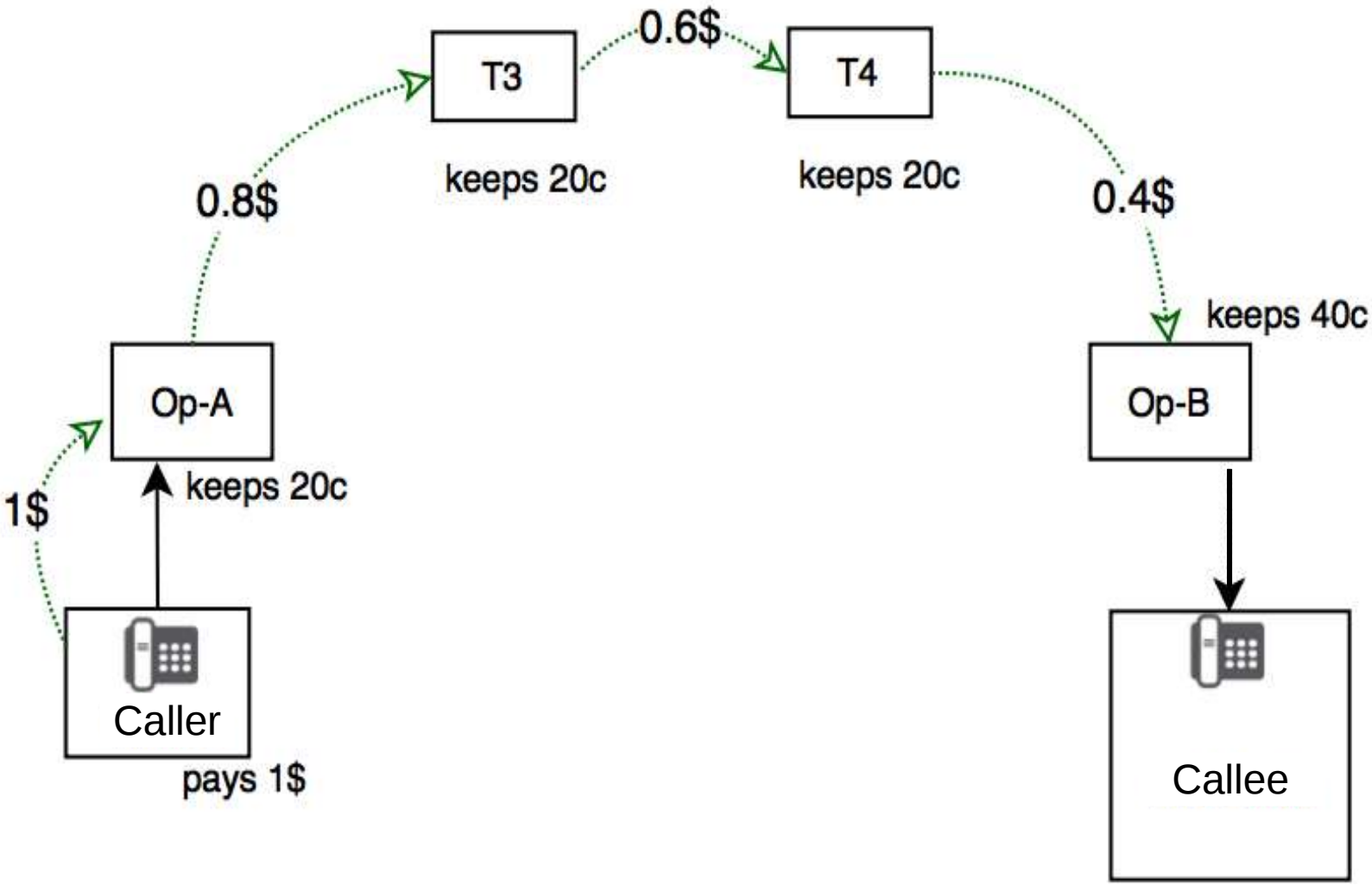
Regular International Call



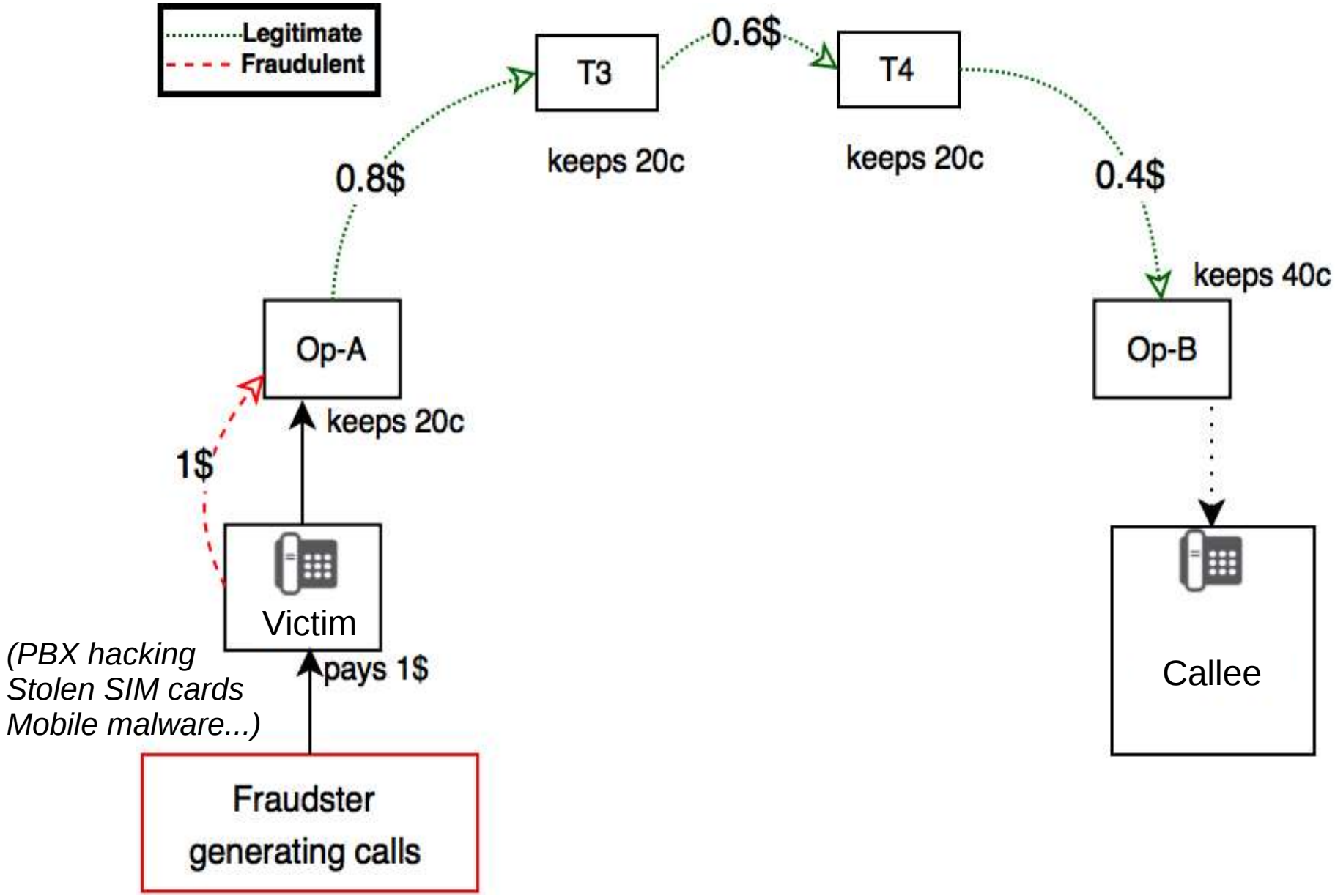
Regular International Call



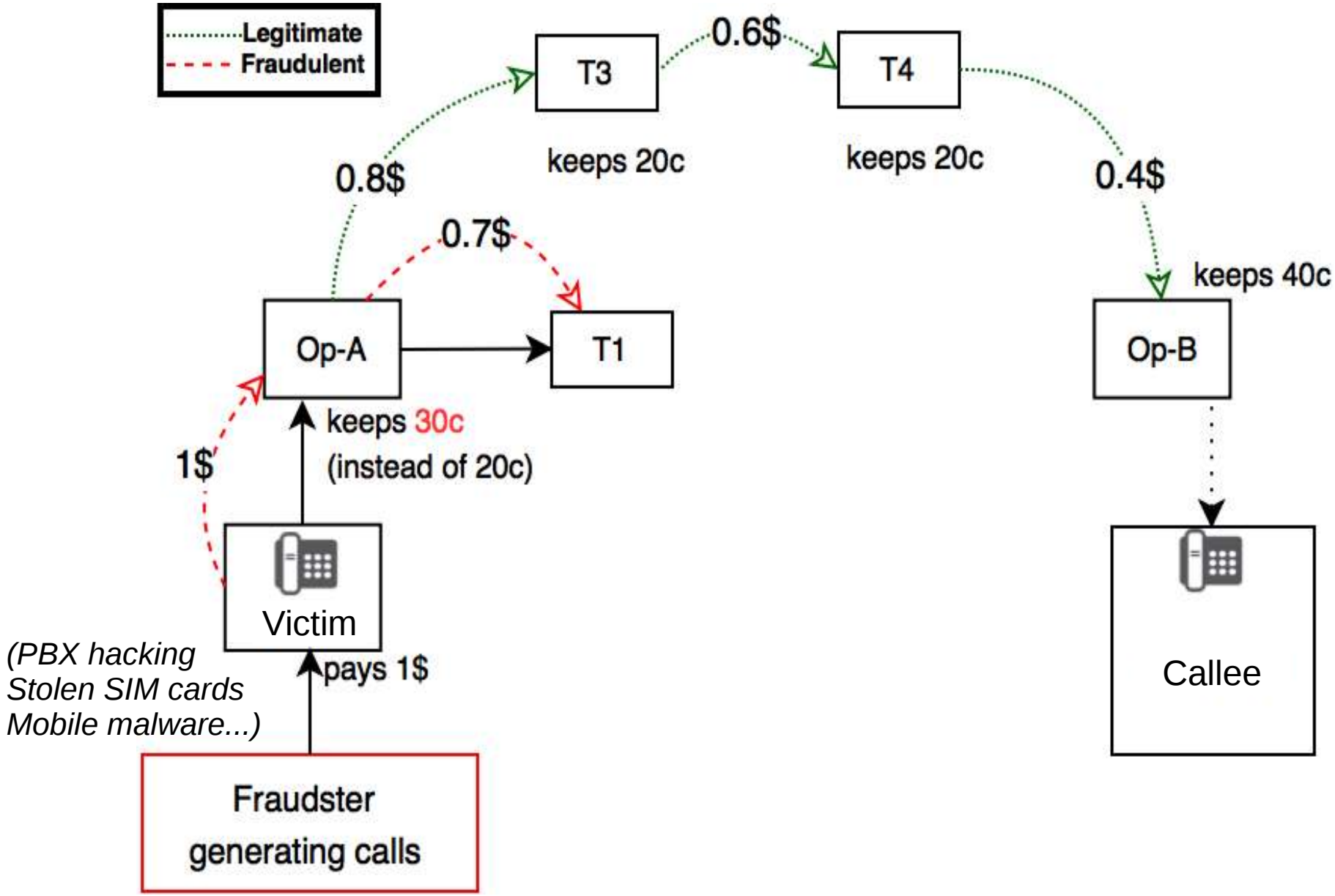
Regular International Call



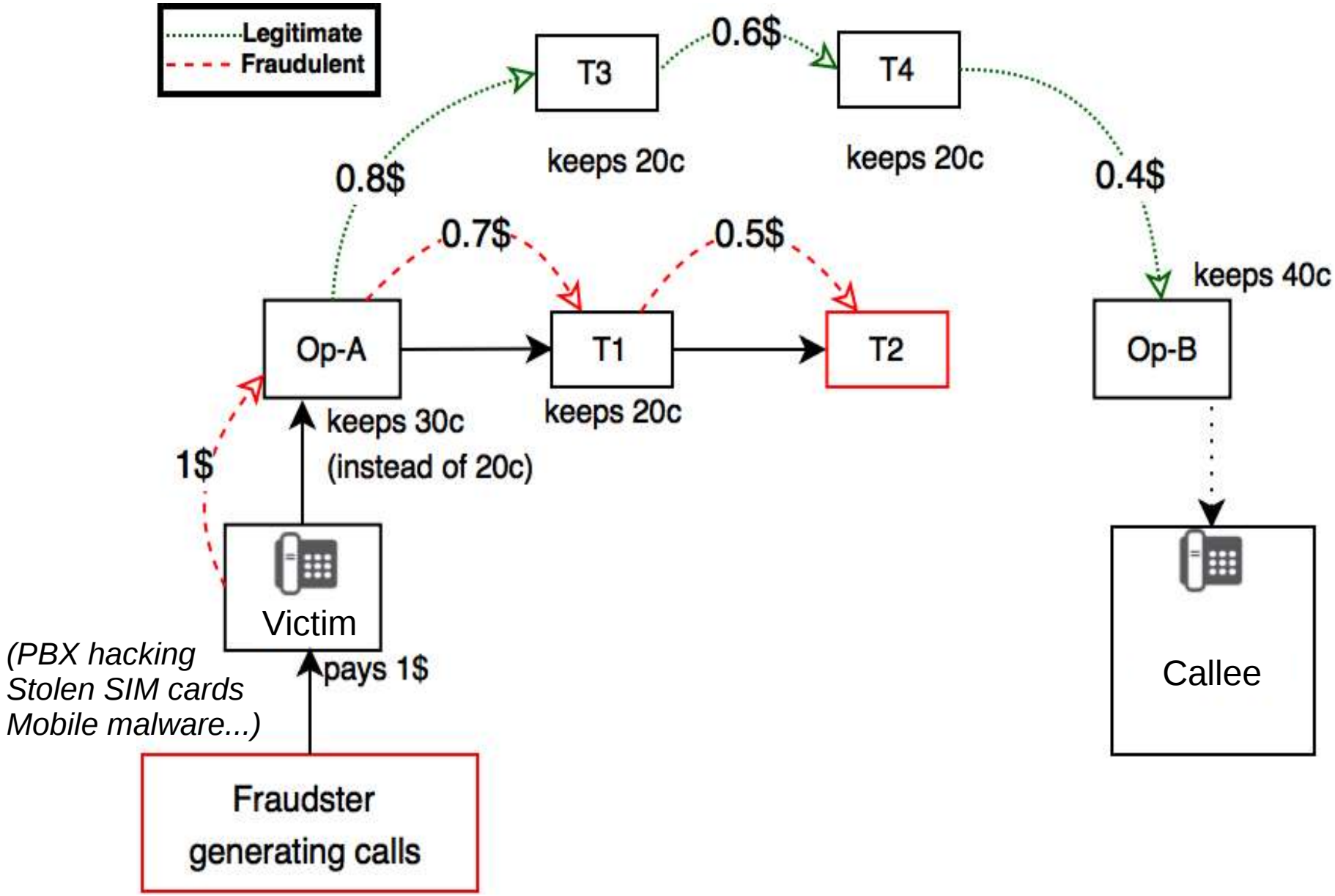
International Revenue Share Fraud



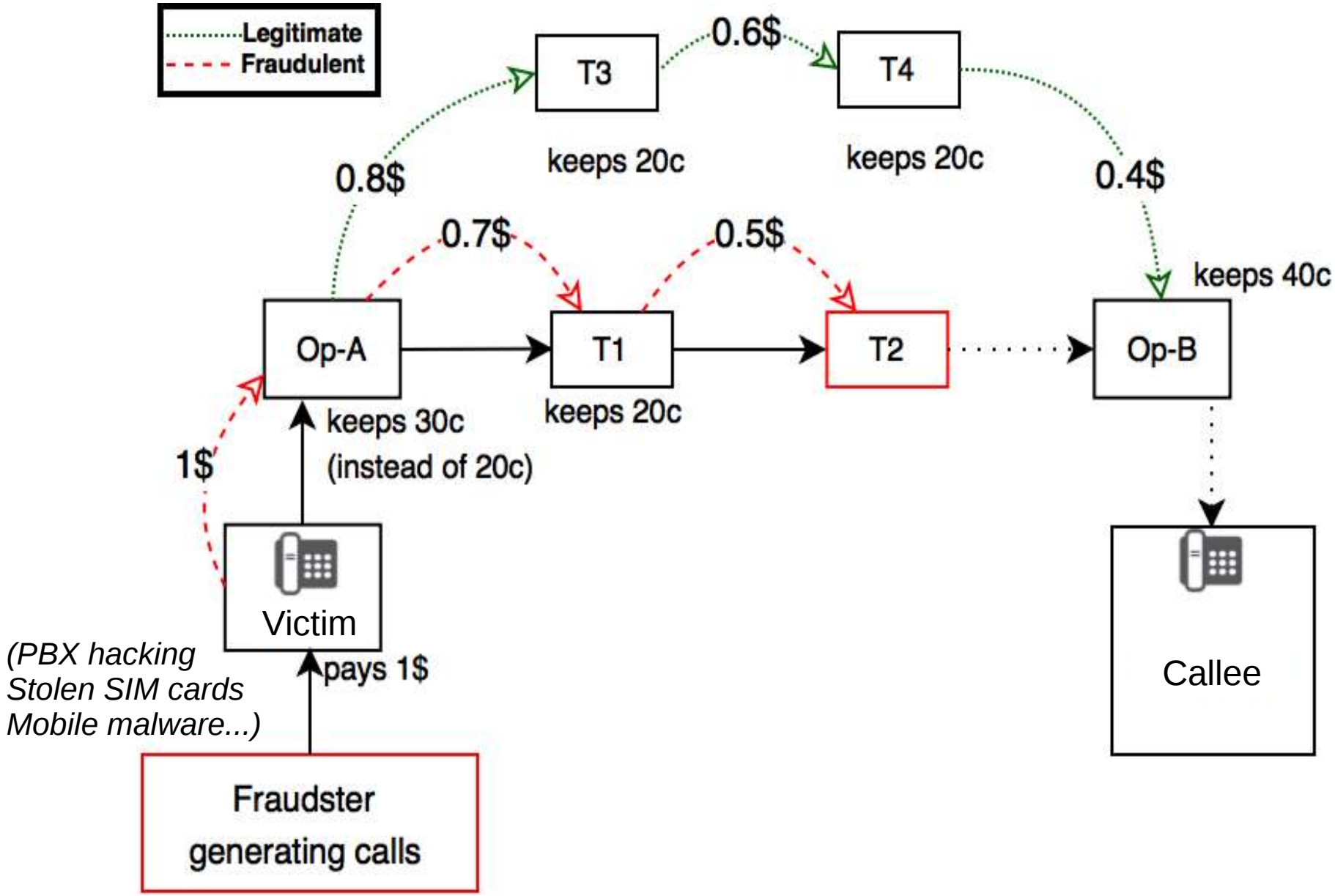
International Revenue Share Fraud



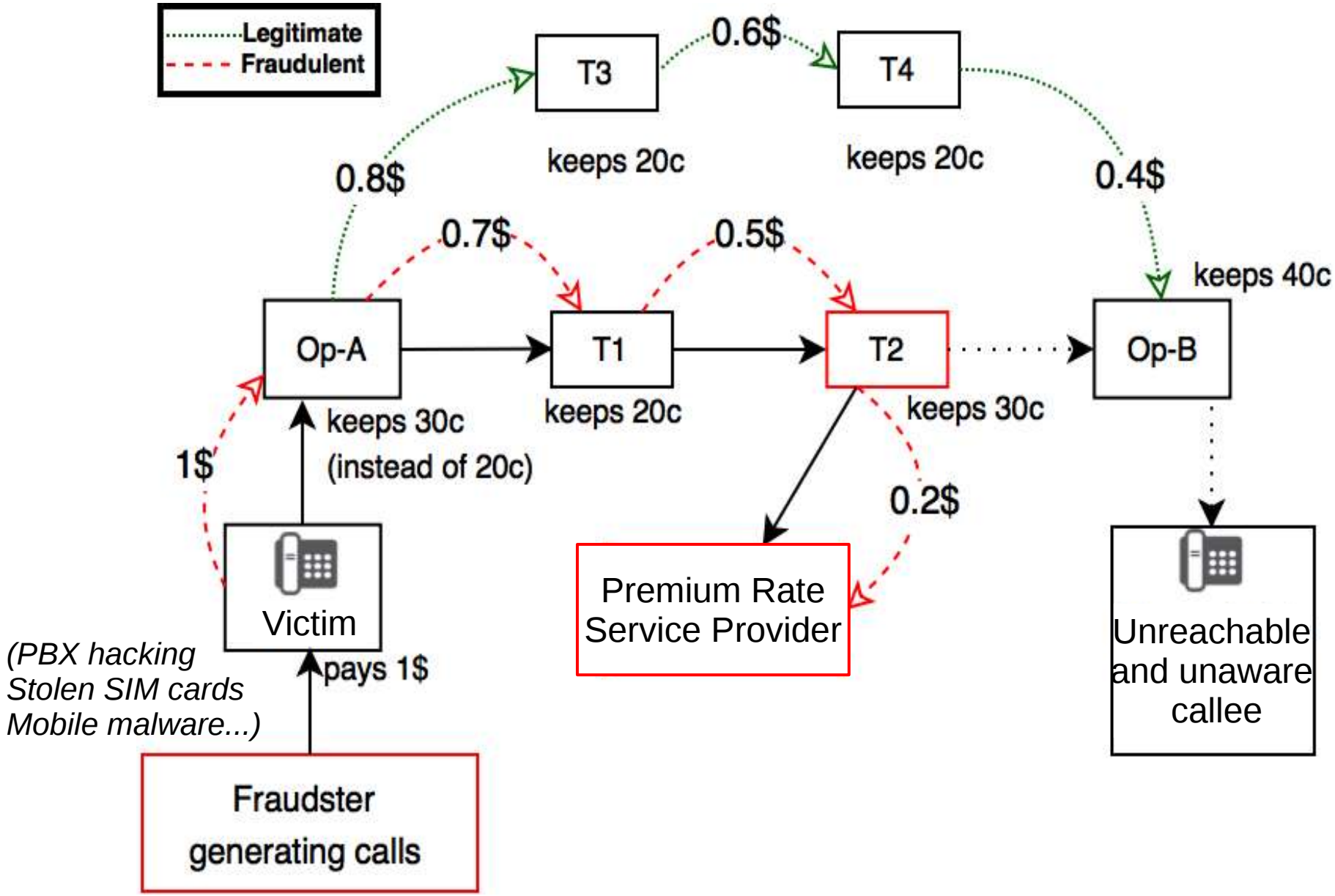
International Revenue Share Fraud



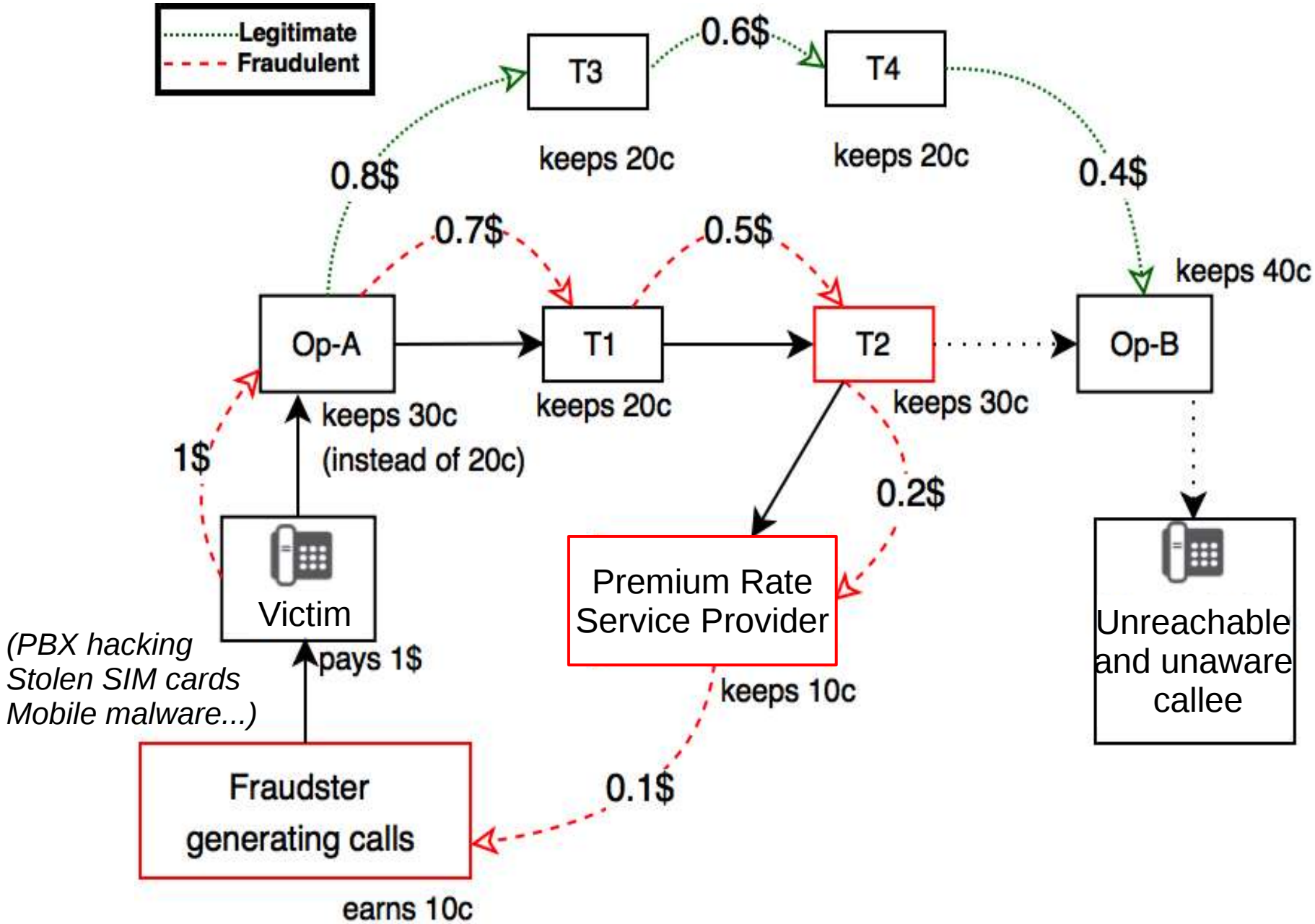
International Revenue Share Fraud



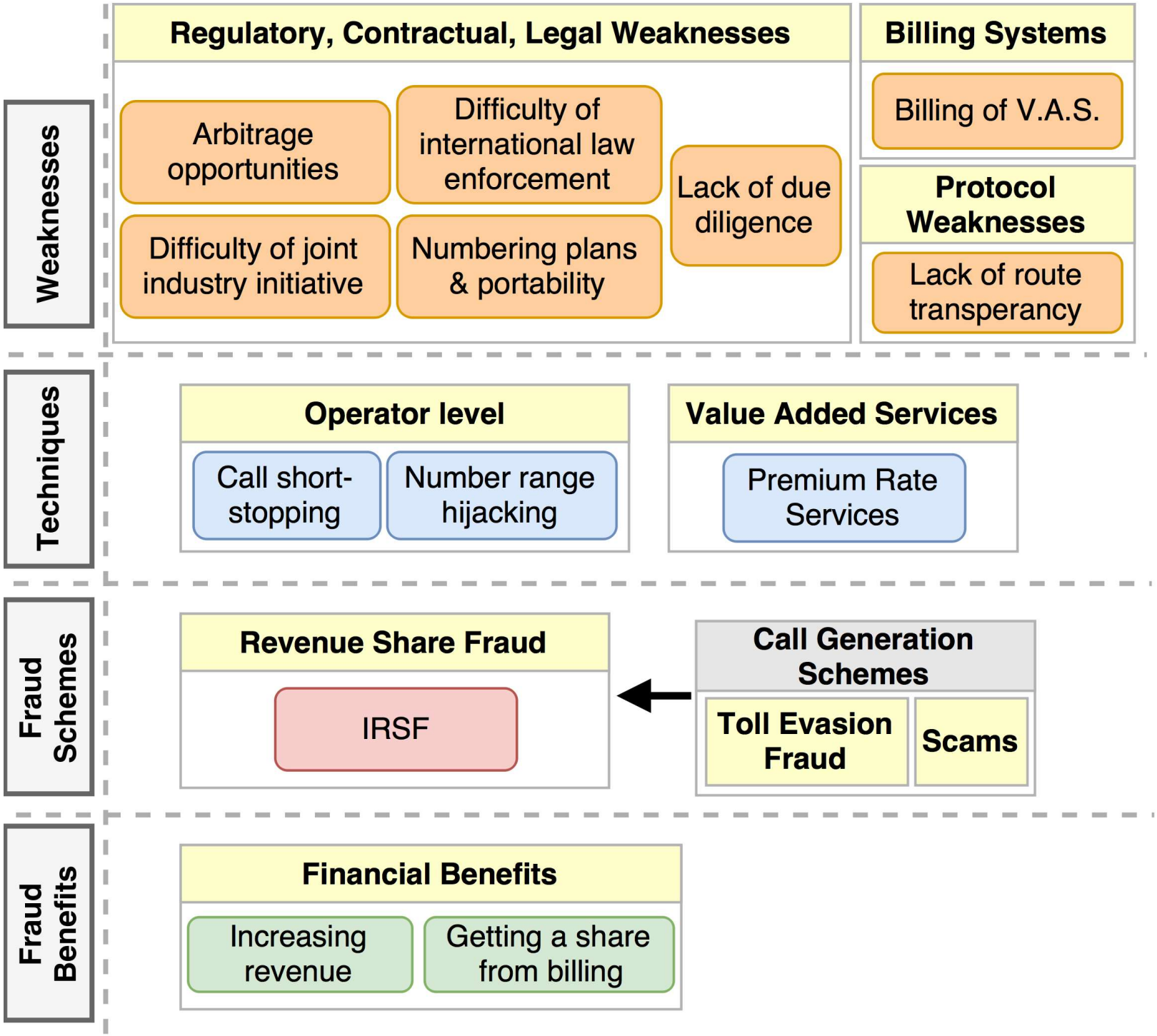
International Revenue Share Fraud



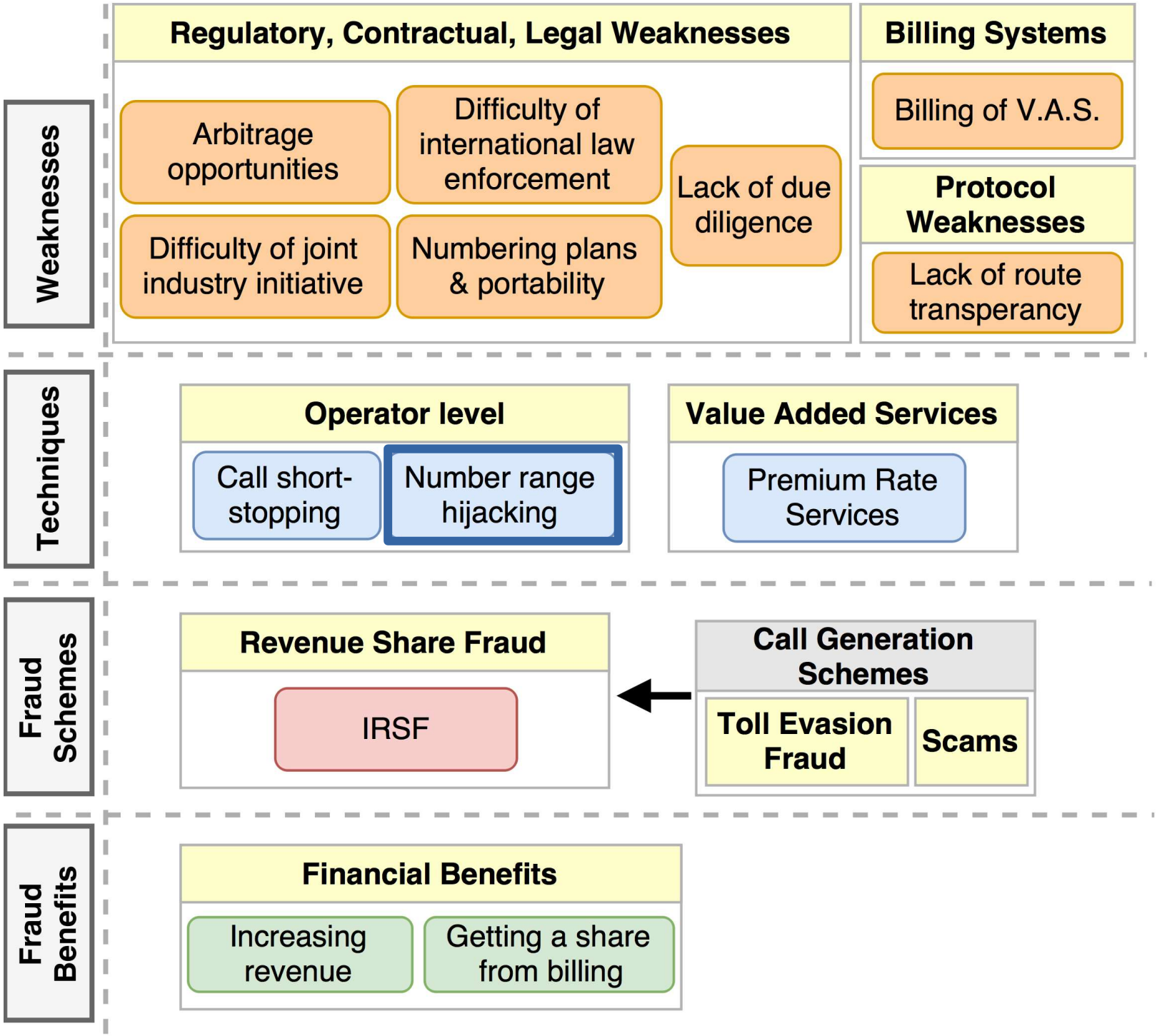
International Revenue Share Fraud



IRSF in fraud taxonomy



IRSF in fraud taxonomy



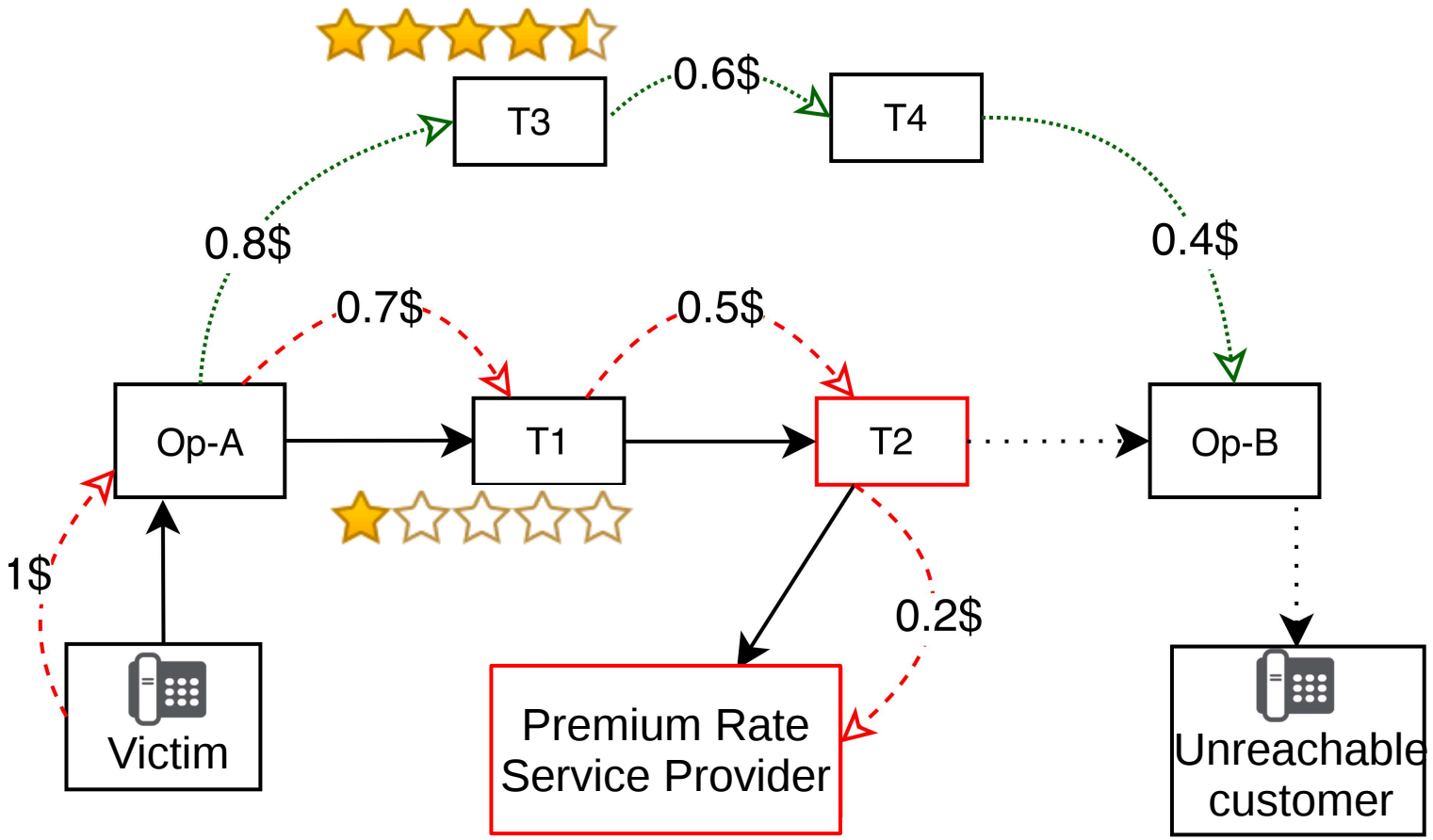
Fraud Scheme: IRSF

Fraud Benefit: Financial

Technique: Number Range Hijacking

- Advertising cheap rates for a number range to attract traffic
- Similar to false BGP prefix advertisements (BGP hijack)

Weakness: Lack of due diligence & Least cost routing policy



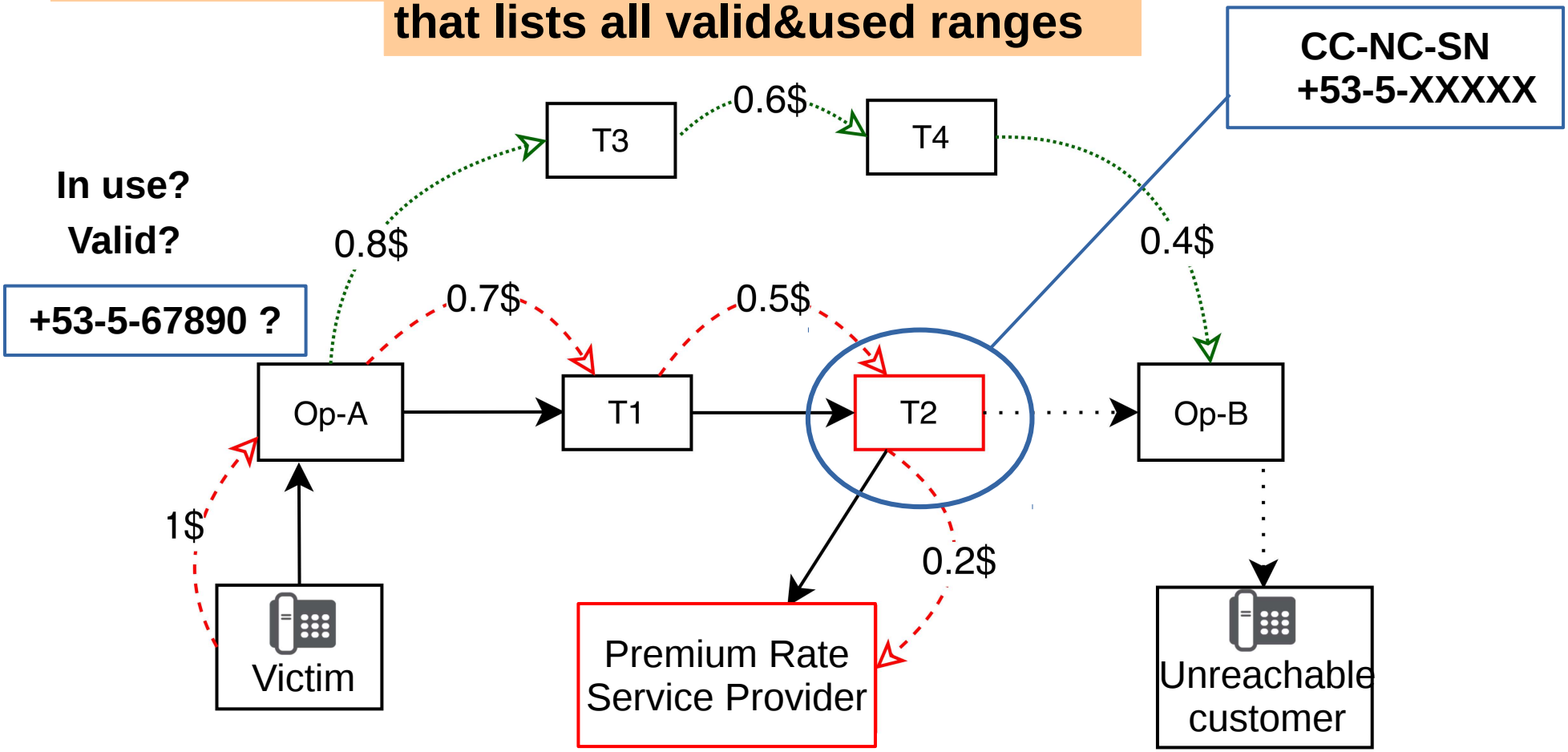
Fraud Scheme: IRSF

Fraud Benefit: Financial

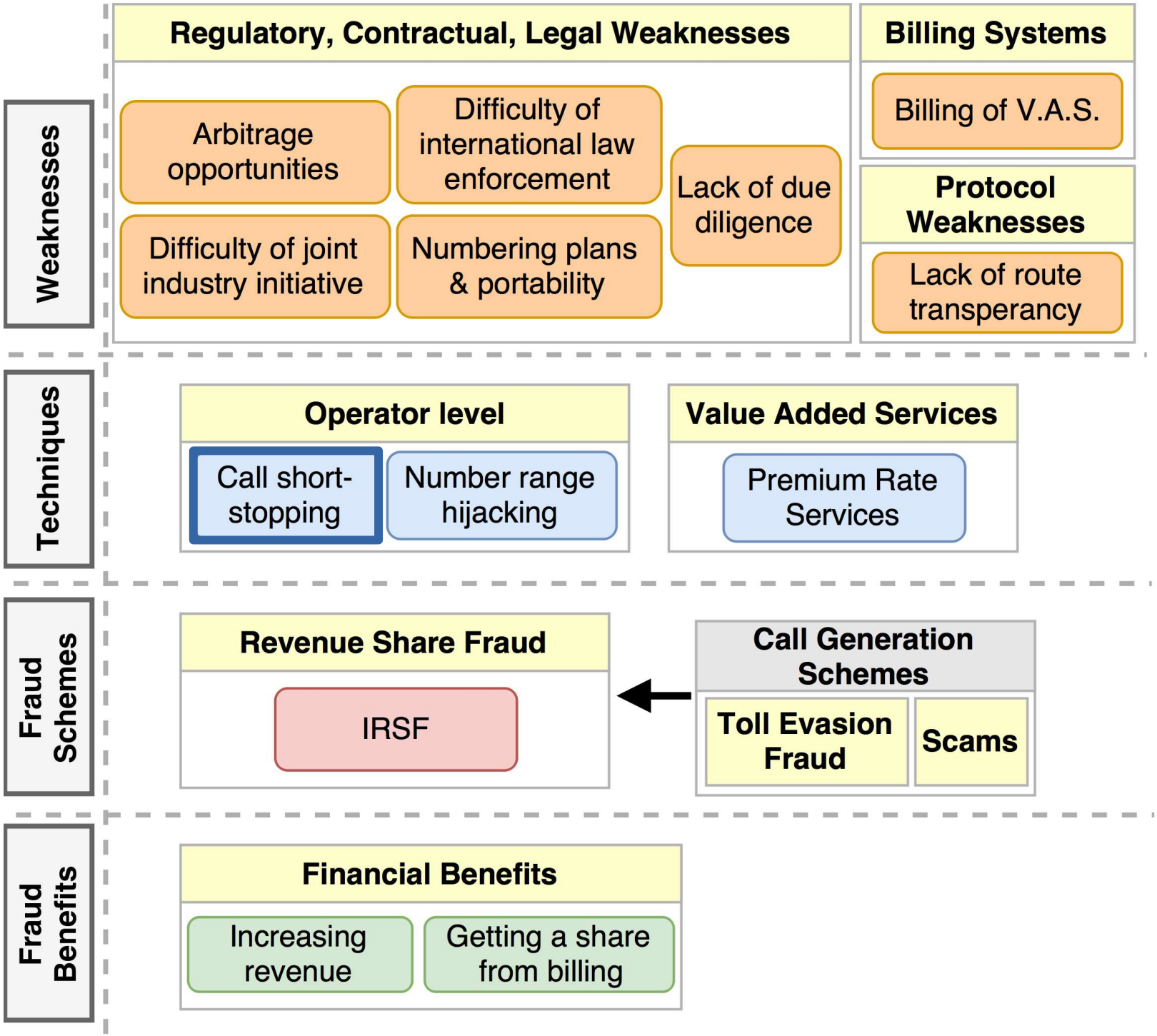
Technique: Number Range Hijacking

- Advertising cheap rates for a number range to attract traffic
- Similar to false BGP prefix advertisements (BGP hijack)

Weakness: Lack of a global numbering plan that lists all valid&used ranges



IRSF in fraud taxonomy



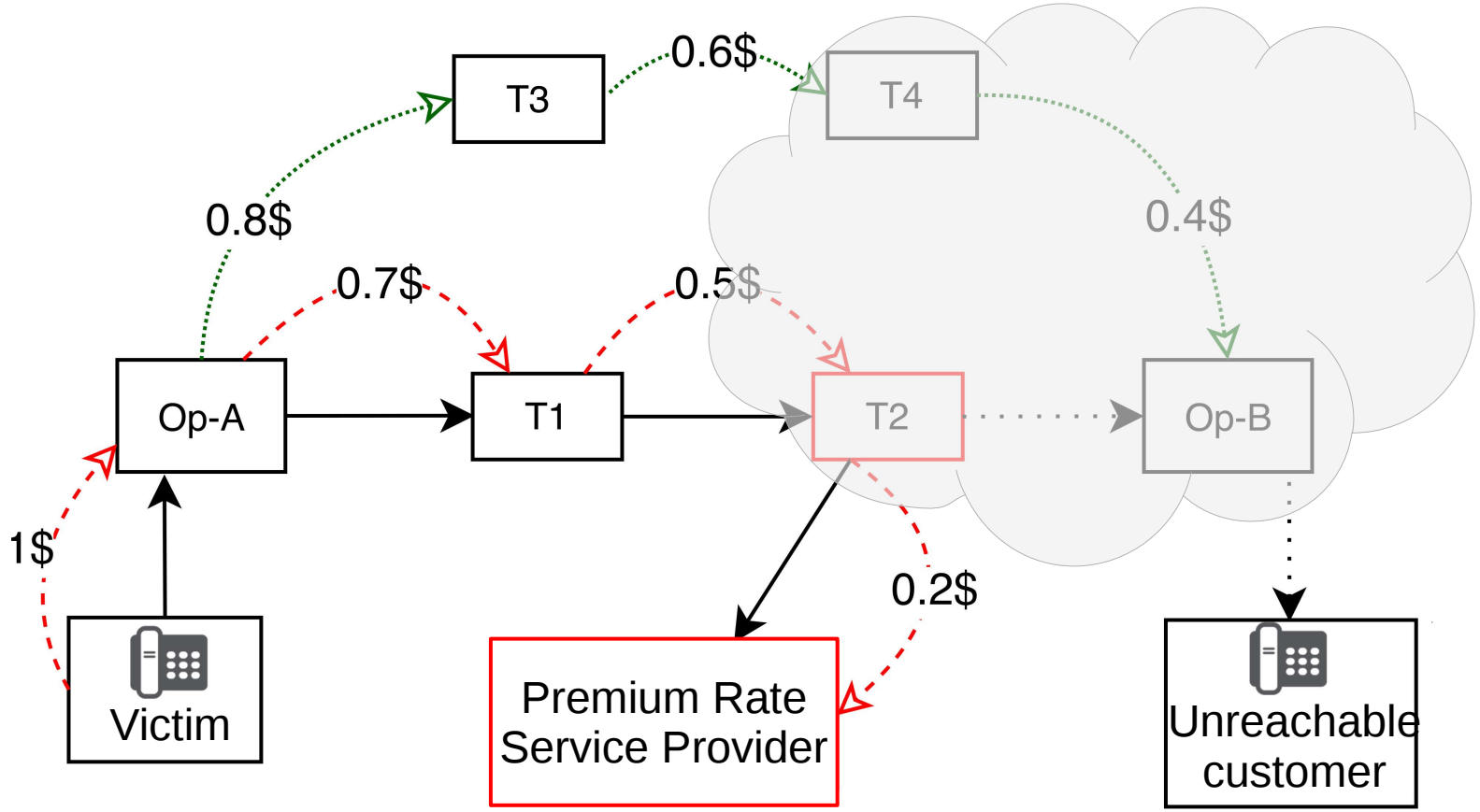
Fraud Scheme: IRSF

Fraud Benefit: Financial

Technique: Call short-stopping

- Manipulation of call routing to terminate (short-stop) the call on a pre-recorded voice message
- Short-stopped calls do not reach the legitimate destination

Weakness: Lack of route transparency



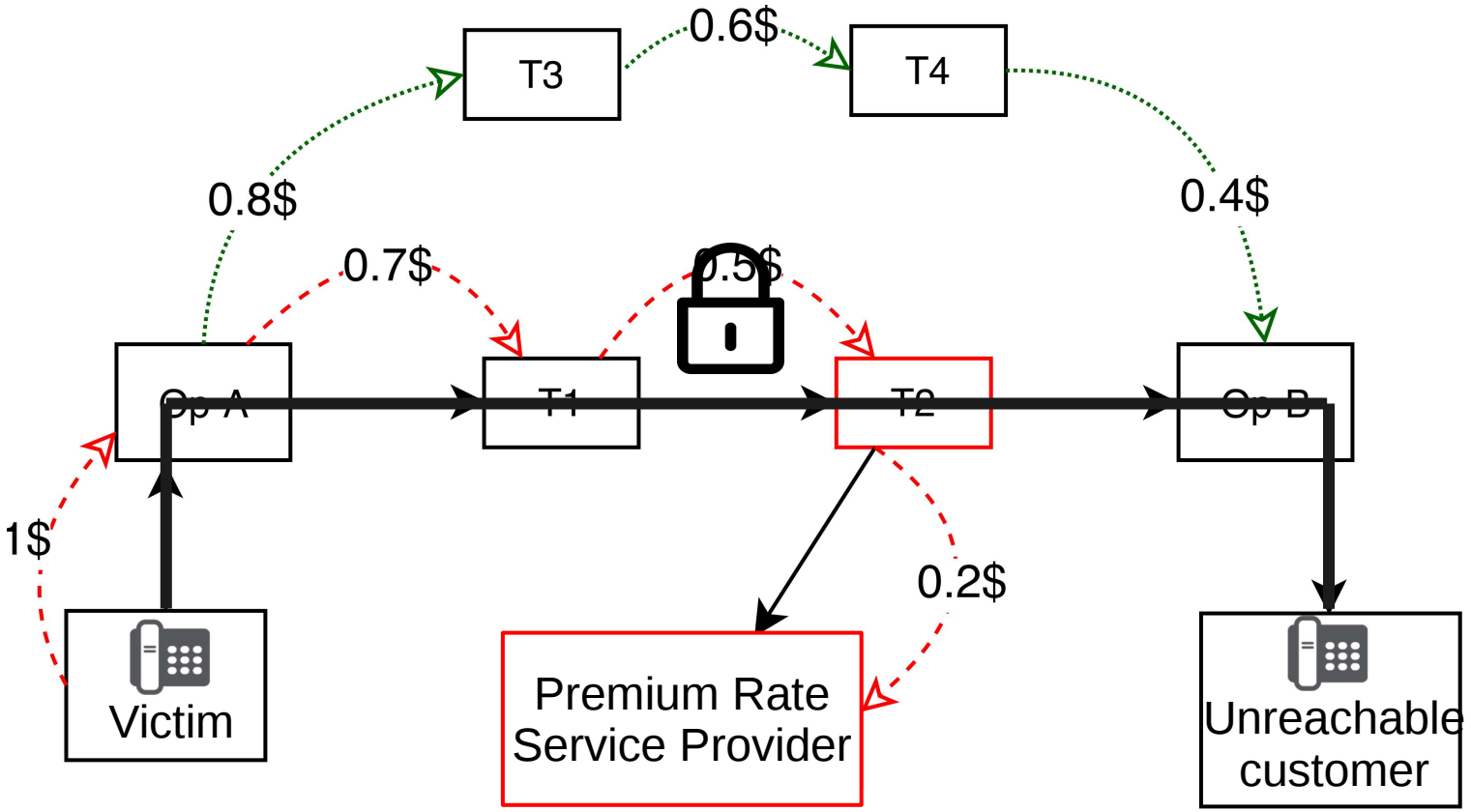
Fraud Scheme: IRSF

Fraud Benefit: Financial

Technique: Call short-stopping

- Manipulation of call routing to terminate (short-stop) the call on a pre-recorded voice message
- Short-stopped calls do not reach the legitimate destination

Weakness: Lack of end-to-end security in call signaling



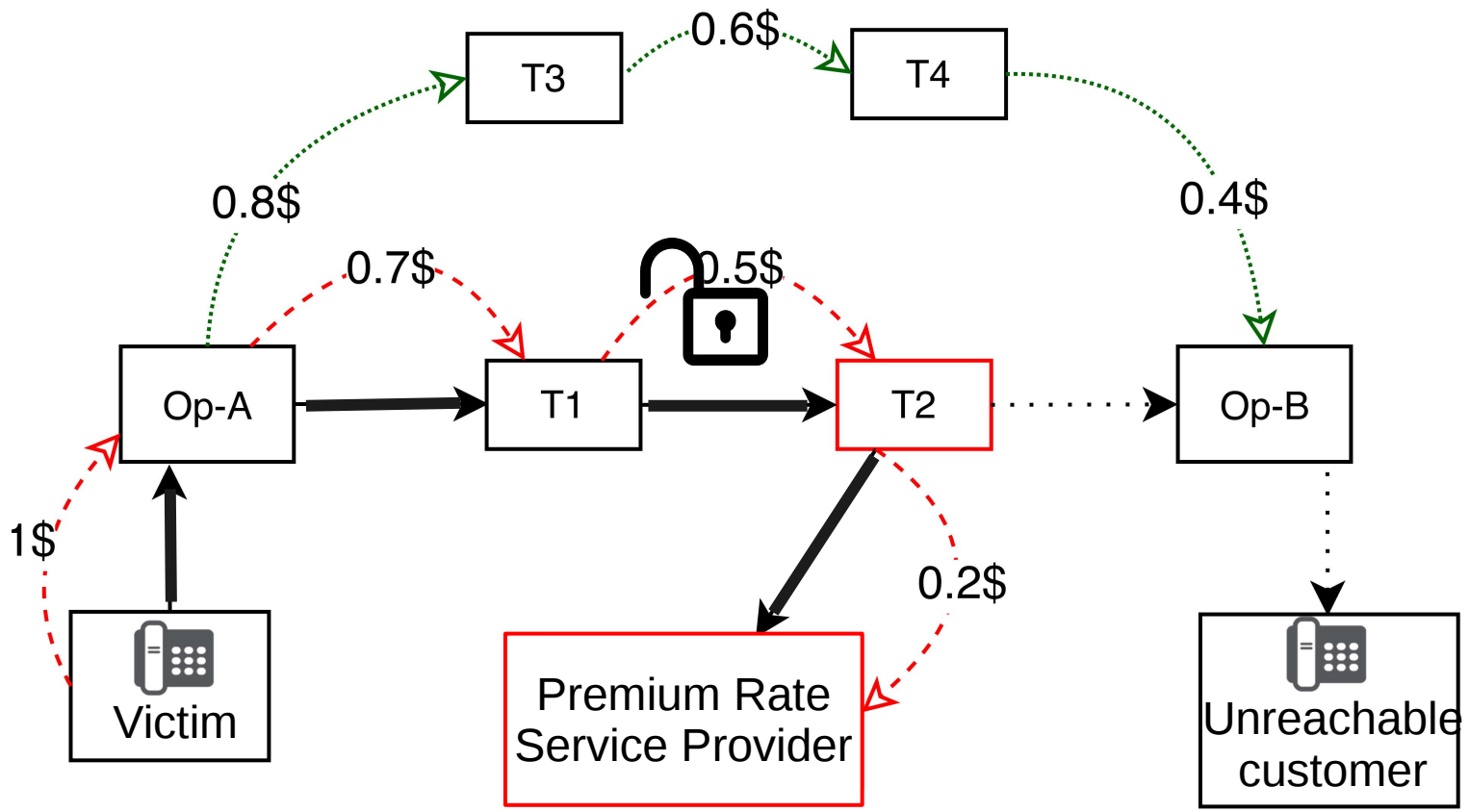
Fraud Scheme: IRSF

Fraud Benefit: Financial

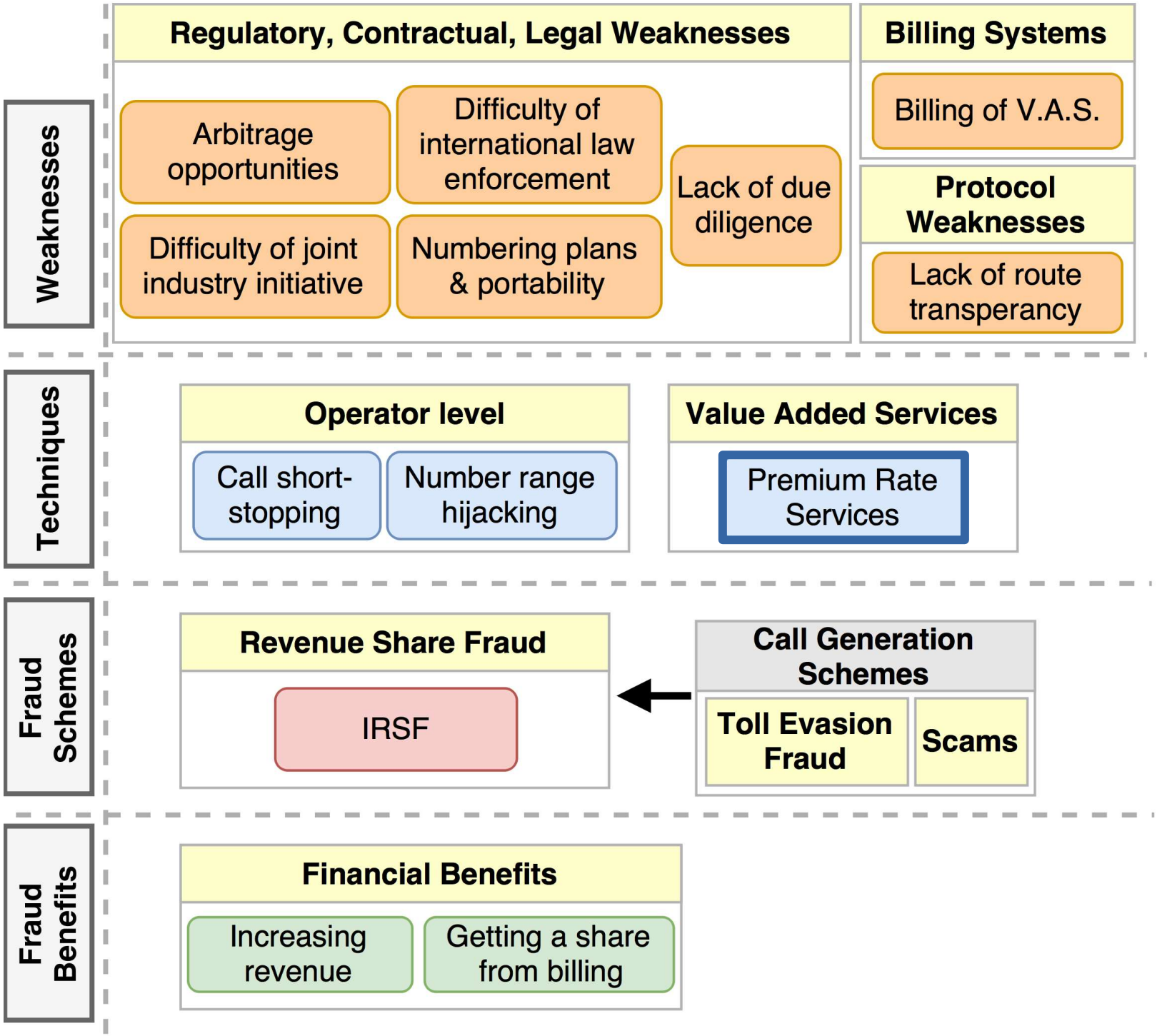
Technique: Call short-stopping

- Manipulation of call routing to terminate (short-stop) the call on a pre-recorded voice message
- Short-stopped calls do not reach the legitimate destination

Weakness: Lack of end-to-end security in call signaling



IRSF in fraud taxonomy



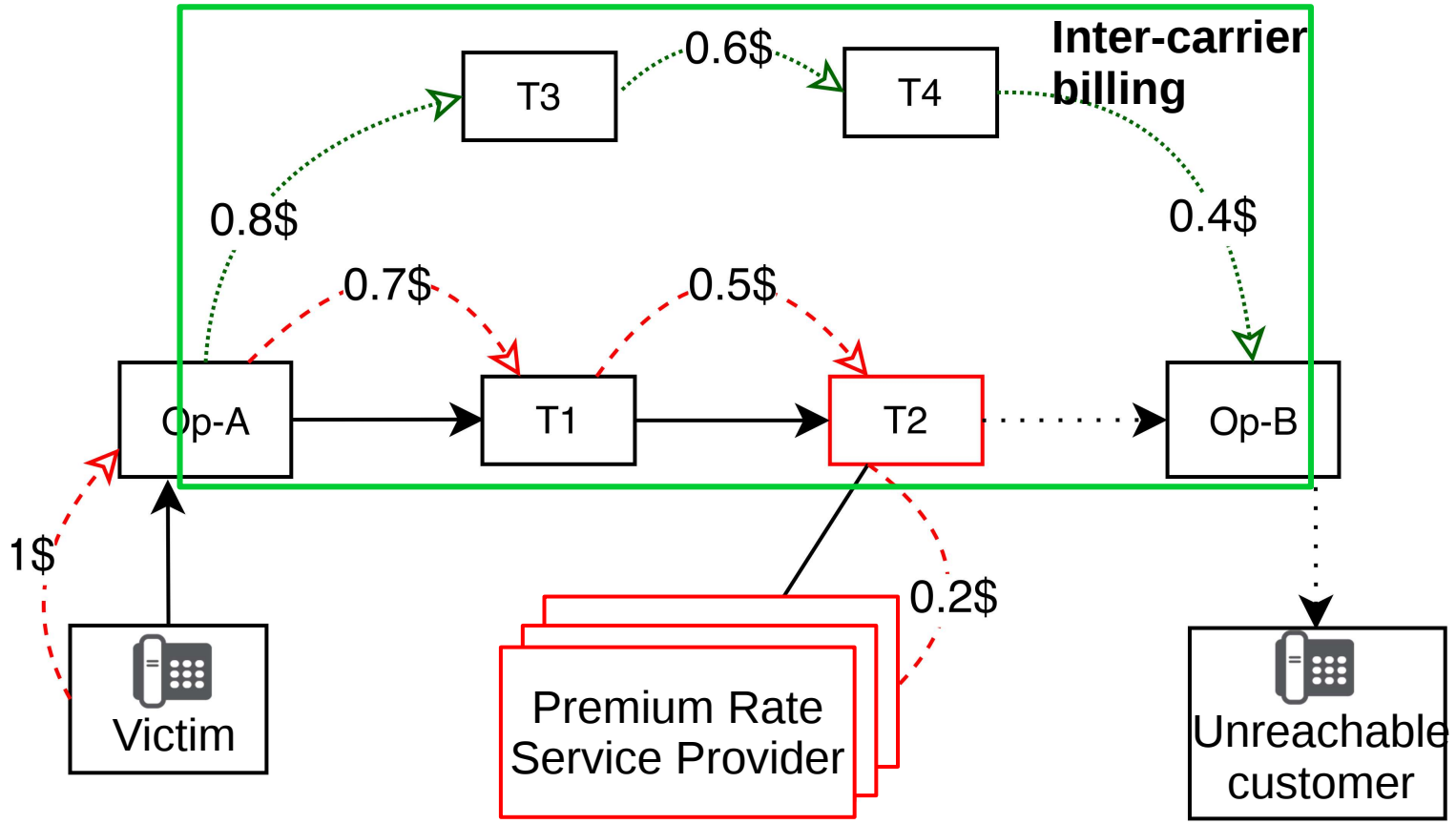
Fraud Scheme: IRSF

Fraud Benefit: Financial

Technique: Premium Rate Services

- Abuse of billing (cash-back) mechanism

Weakness: Complexity of billing systems



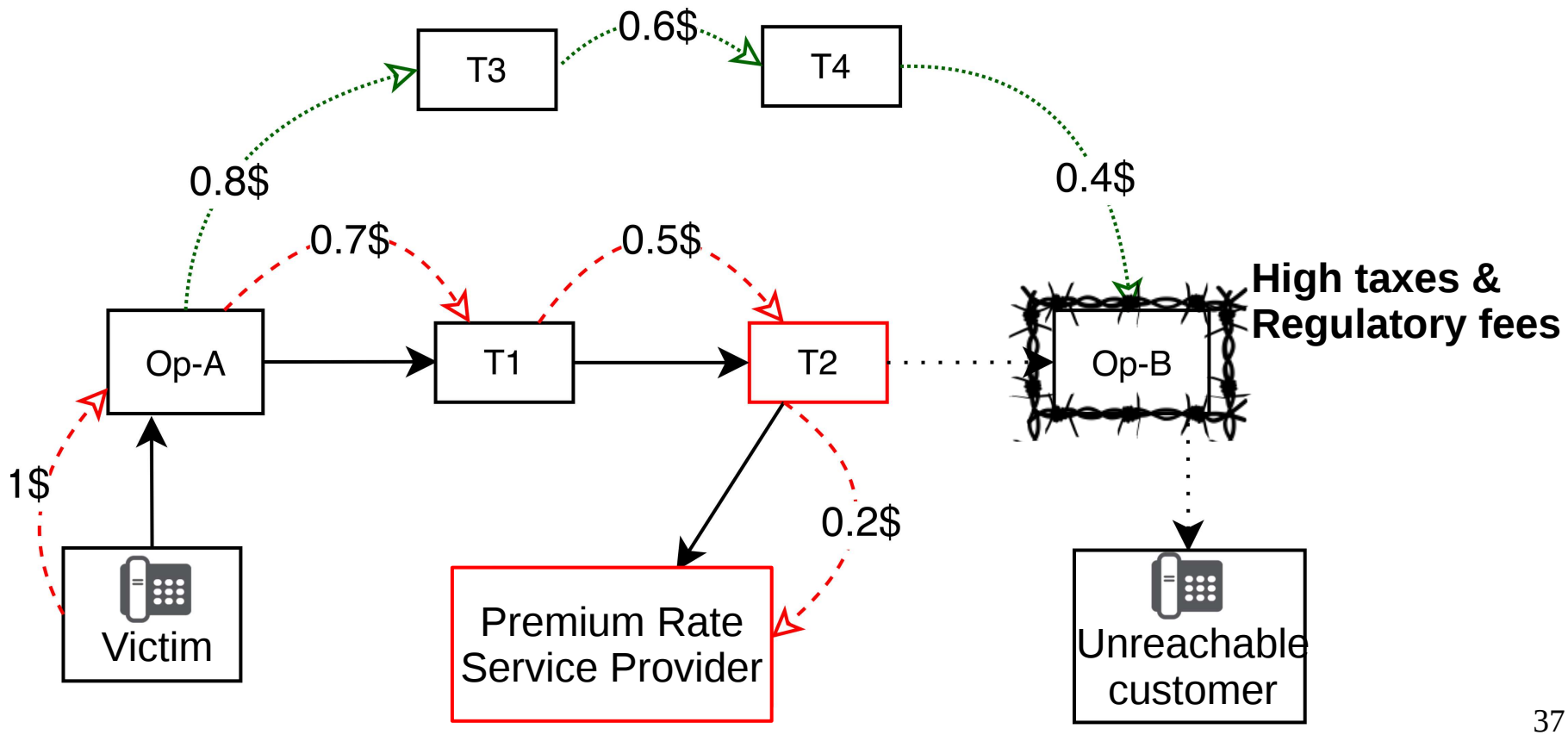
Fraud Scheme: IRSF

Fraud Benefit: Financial

Technique: Premium Rate Services

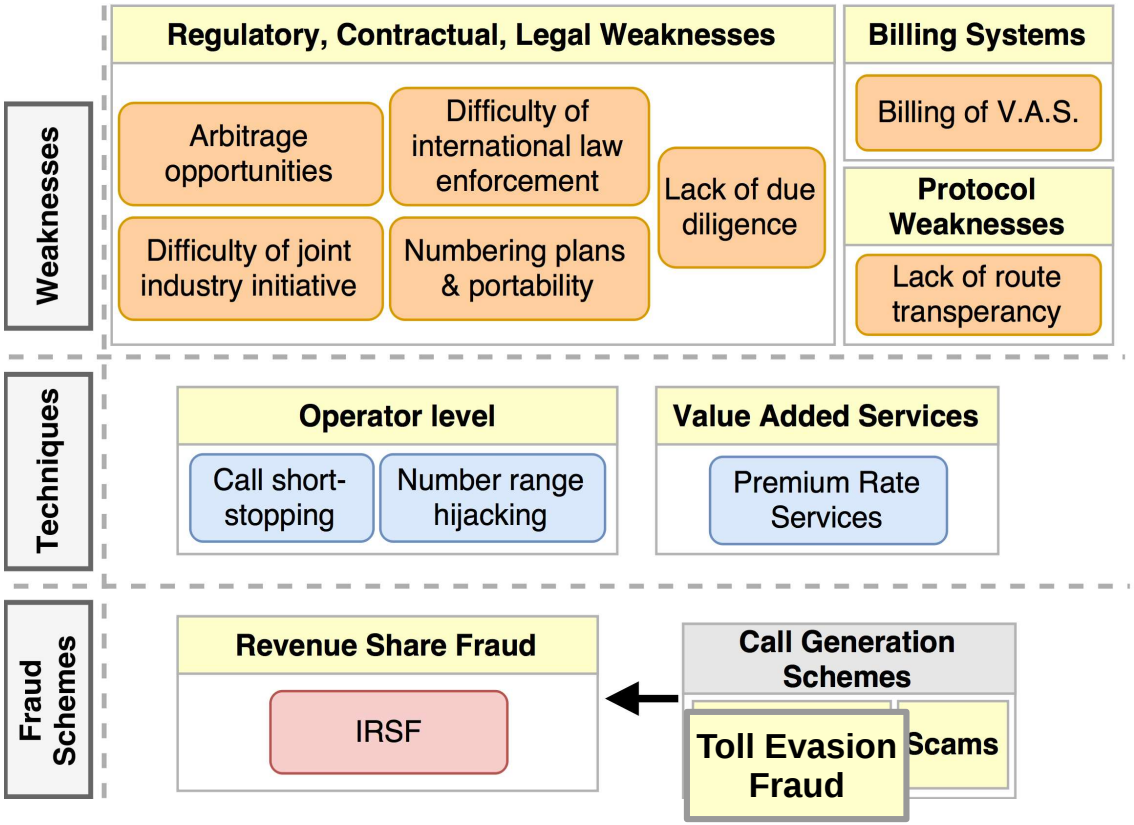
- Abuse of billing (cash-back) mechanism
- Abuse of expensive destinations as pseudo “international premium rate numbers” *(Legitimate allocation: +979 range)*

Weakness: Variety of regulation and laws



Addressing IRSF?

- Initially, call generation was performed by using fraudulently obtained SIM cards in roaming
  - Weakness: Late availability of roaming call data records
- Solution proposed:
  Near Real Time Roaming Data Exchange (NRTRDE) systems



Addressing IRSF

- Initially, call generation was performed by using fraudulently obtained SIM cards in roaming
  - Weakness: Late availability of roaming call data records
- Solution proposed: Near Real Time Roaming Data Exchange (NRTRDE) systems

➡ Only a countermeasure for one type of call generation

➡ Real weaknesses manipulated by IRSF are not addressed

Addressing IRSF

- Initially, call generation was performed by using fraudulently obtained SIM cards in roaming
  - Weakness: Late availability of roaming call data records
- Solution proposed: Near Real Time Roaming Data Exchange (NRTRDE) systems

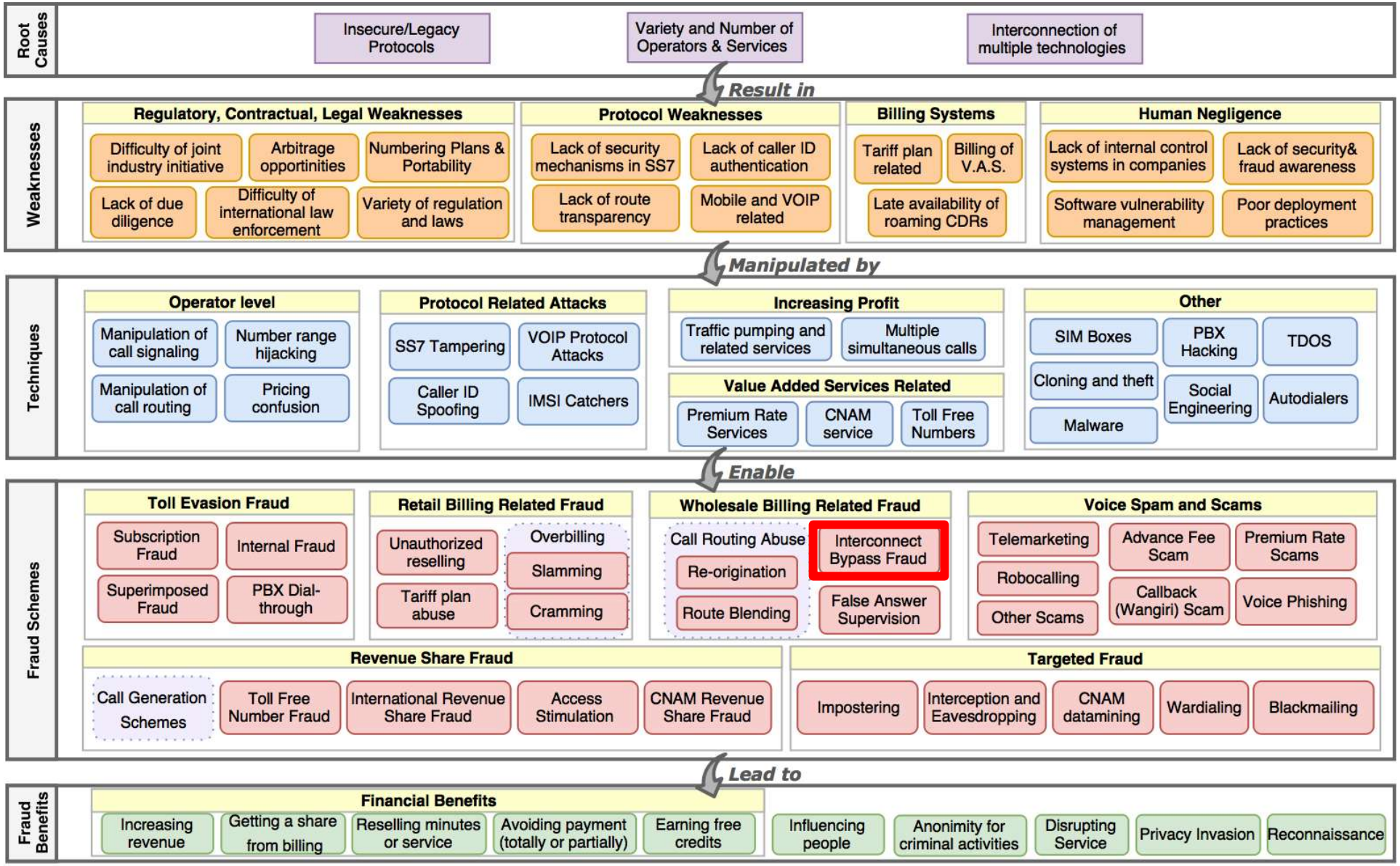
➡ Only a countermeasure for one type of call generation

➡ Real weaknesses manipulated by IRSF are not addressed

- IRSF is still an unsolved problem
  – $10.76 Billion estimated loss in 2015*

[*] CFCA Global Fraud Loss Survey, 2015

Example: Interconnect Bypass Fraud



Interconnect Bypass Fraud

- Use of illegitimate gateway exchanges to avoid the legitimate gateways and international termination fees
  - Example: SIM Boxes and VOIP gateways are frequently used to bypass international part of the calls and terminate them as domestic calls

- $5.97 Billion annual estimated loss*
- **Over-The-Top (OTT) Bypass** is a recent form of interconnect bypass fraud, performed via OTT services

[*]CFCA Global Fraud Loss Survey, 2015

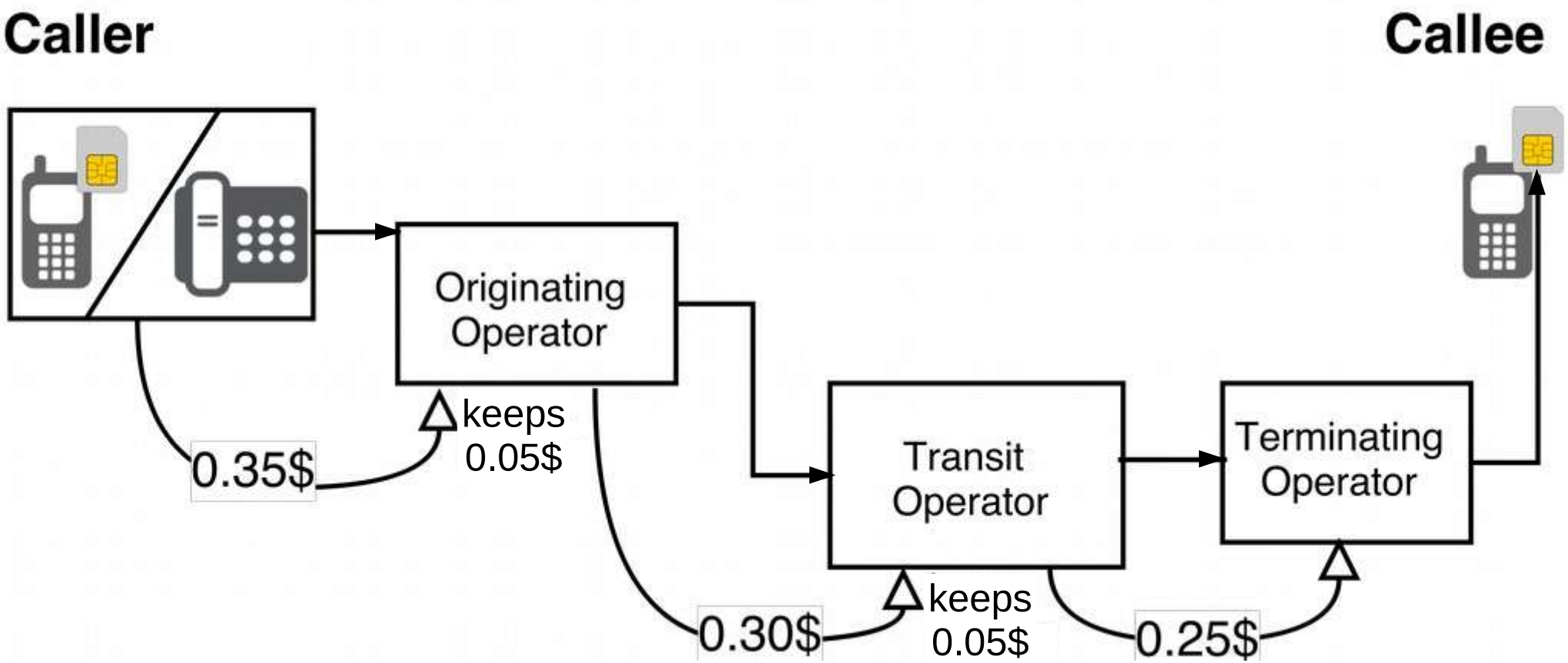
Over-The-Top (OTT) Communications

- Online services that
  - run 'on top of' the operator
  - substitute/compete with traditional telecommunications services
- Global presence through smartphone application markets
- **2 billion OTT messaging users estimated by 2018** [eMarketer'15]

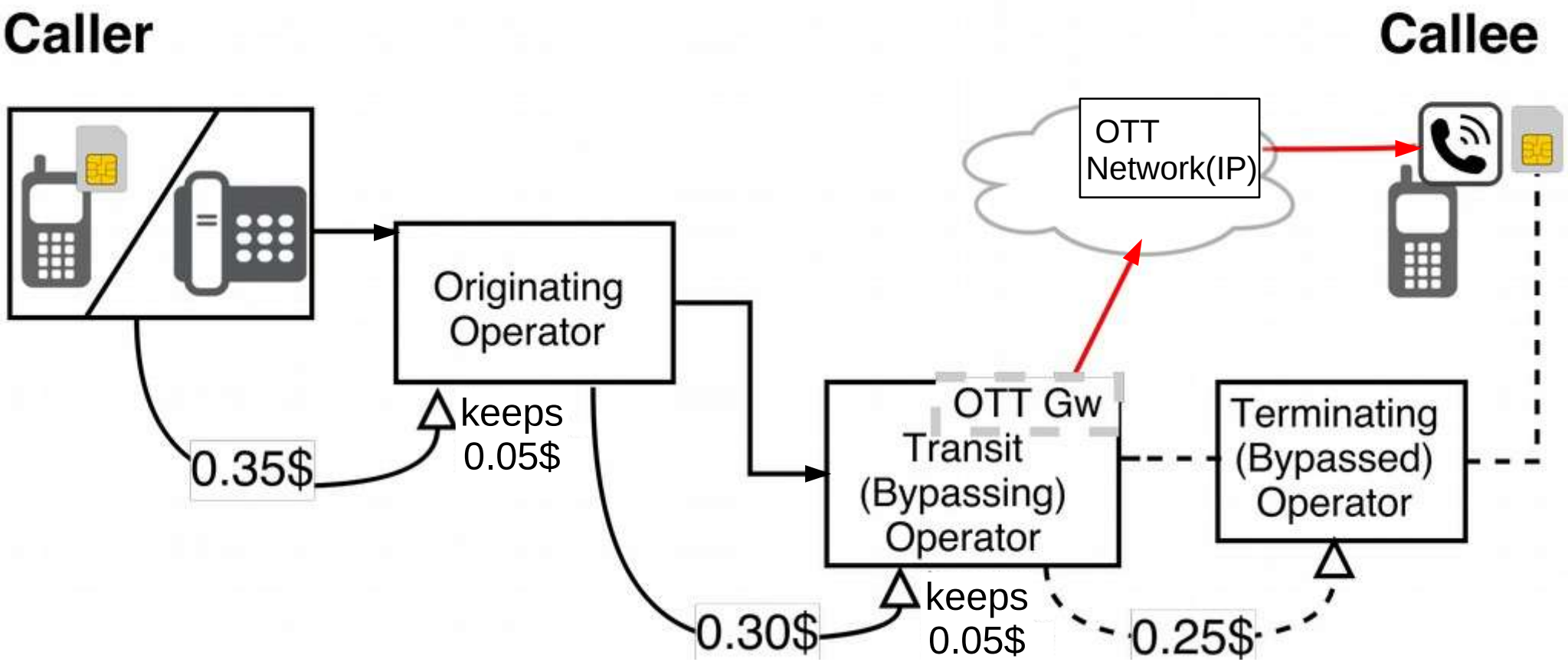
Over-The-Top (OTT) Communications

- **Phone numbers often used for user identification**
- **Terms of use** and default application settings
- **OTT needs revenue:**
  - Advertisement
  - Stickers, games etc.
  - **Telephony interaction**
    - e.g., Skype-in
      Skype-out ☺
    - OTT bypass ☹

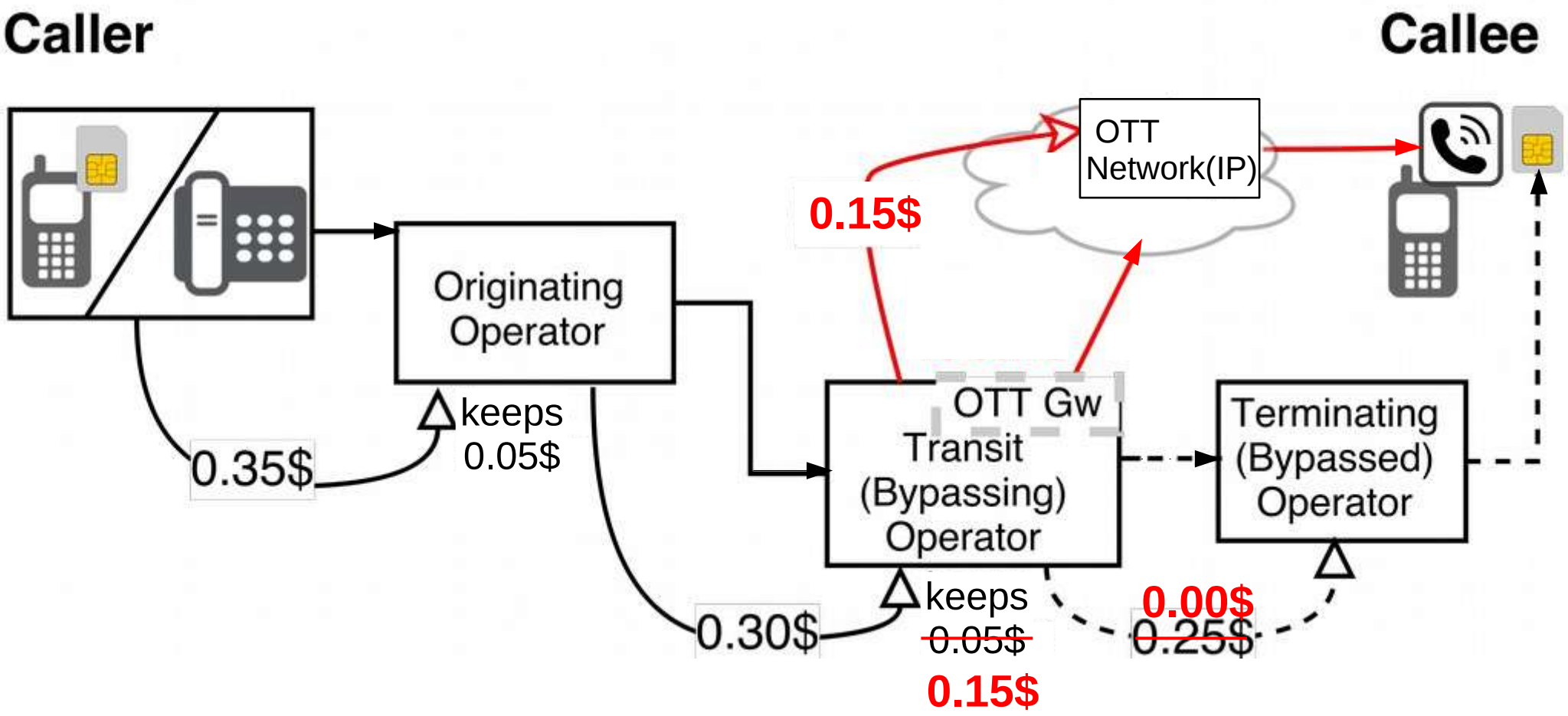
Regular International Call



OTT Bypass Call

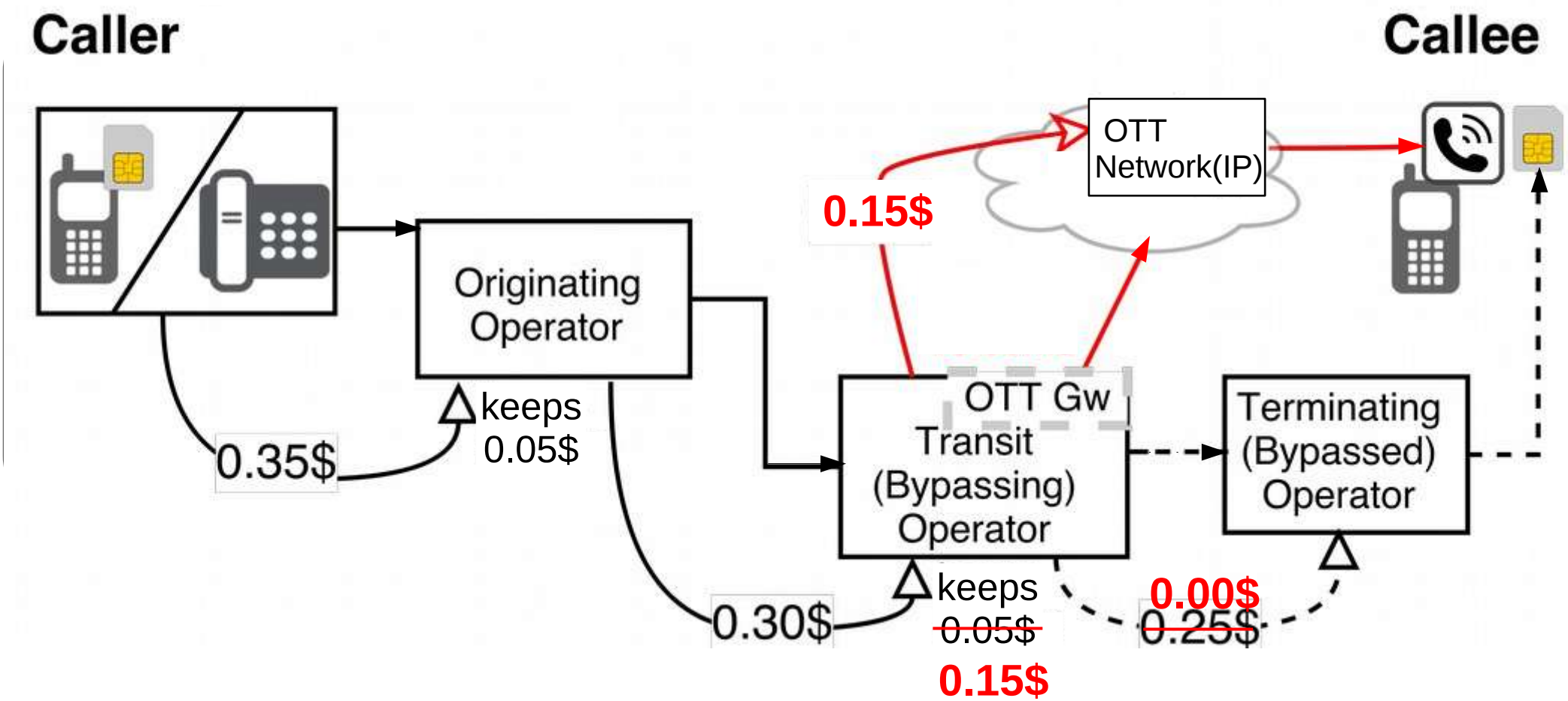


OTT Bypass Call



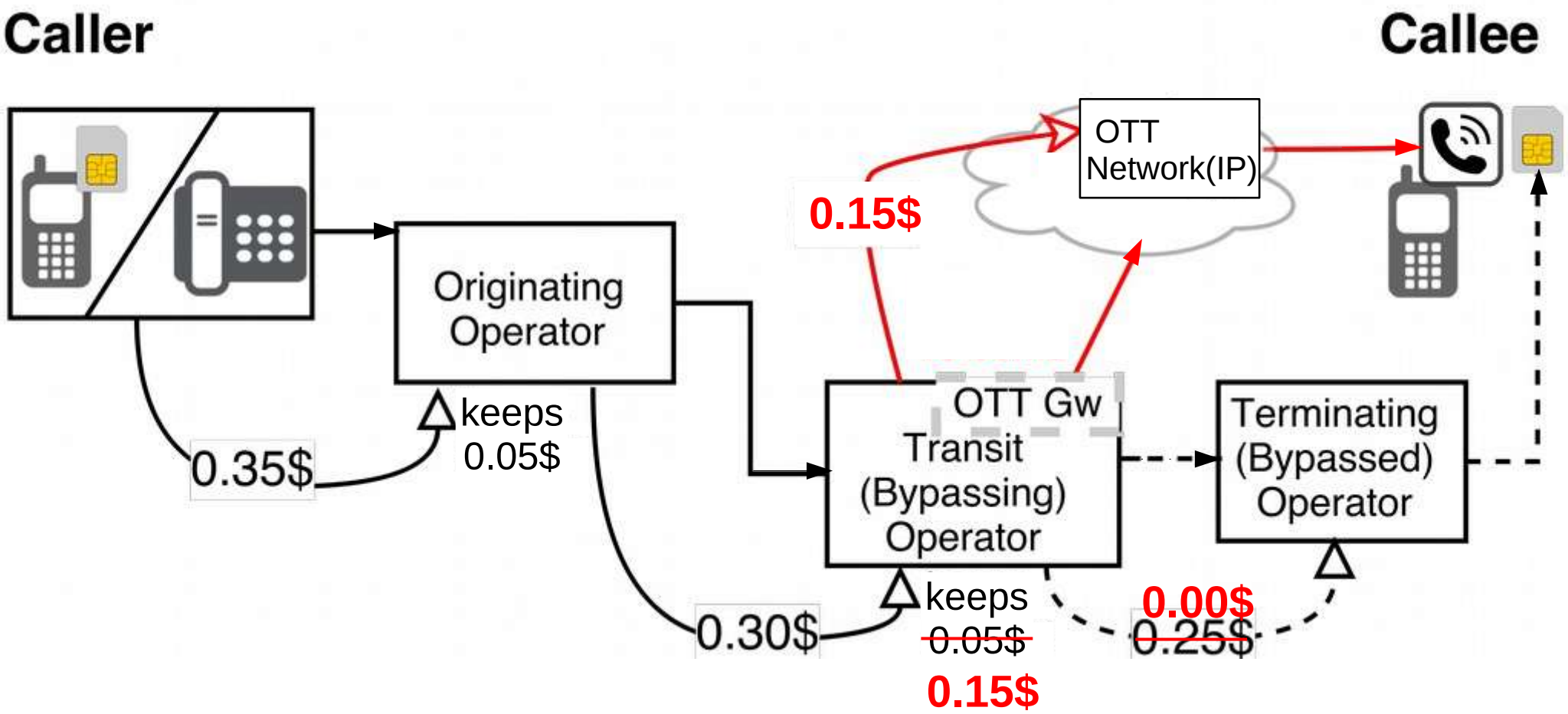
OTT Bypass Call

- *Pays for premium quality (SLA)*
- *Potential quality problems*

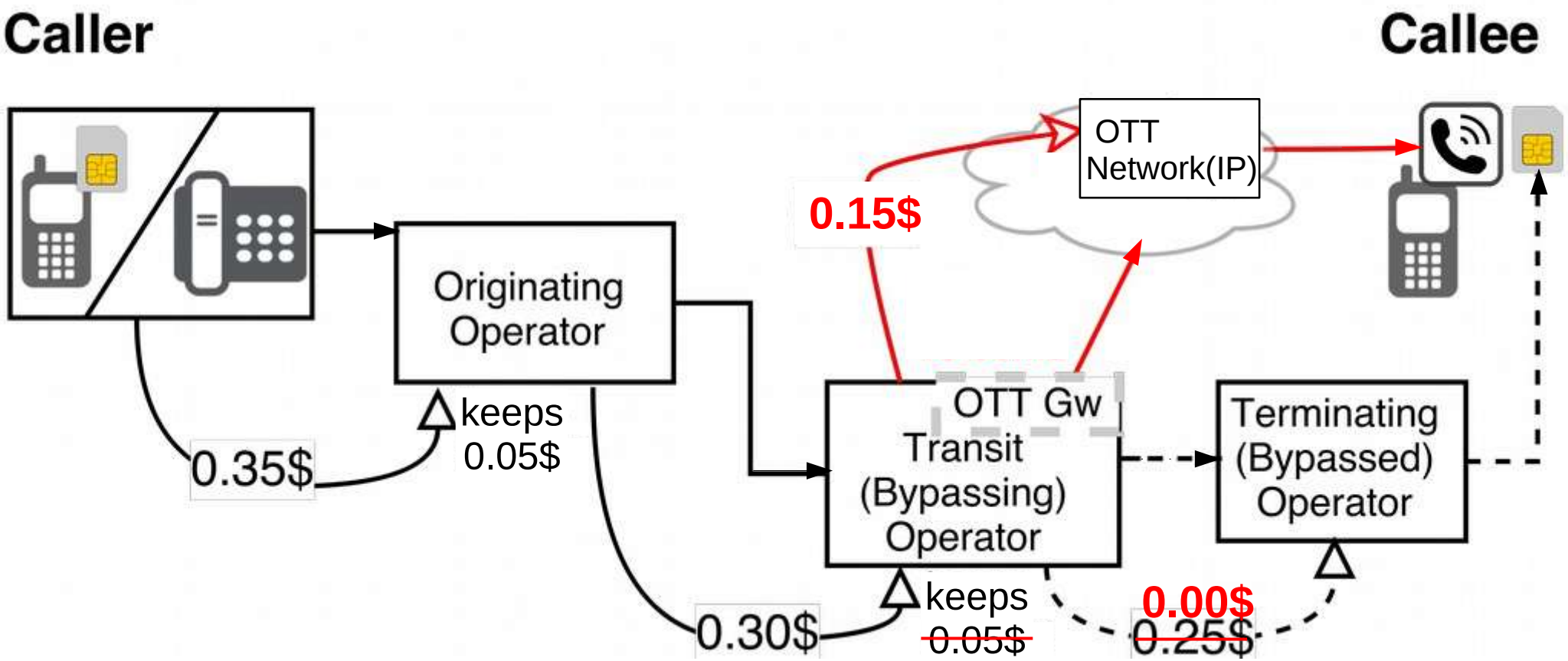


OTT Bypass Call

- Potential quality problems
- May pay for IP traffic
- Cannot use telco services (voicemail, call forwarding)

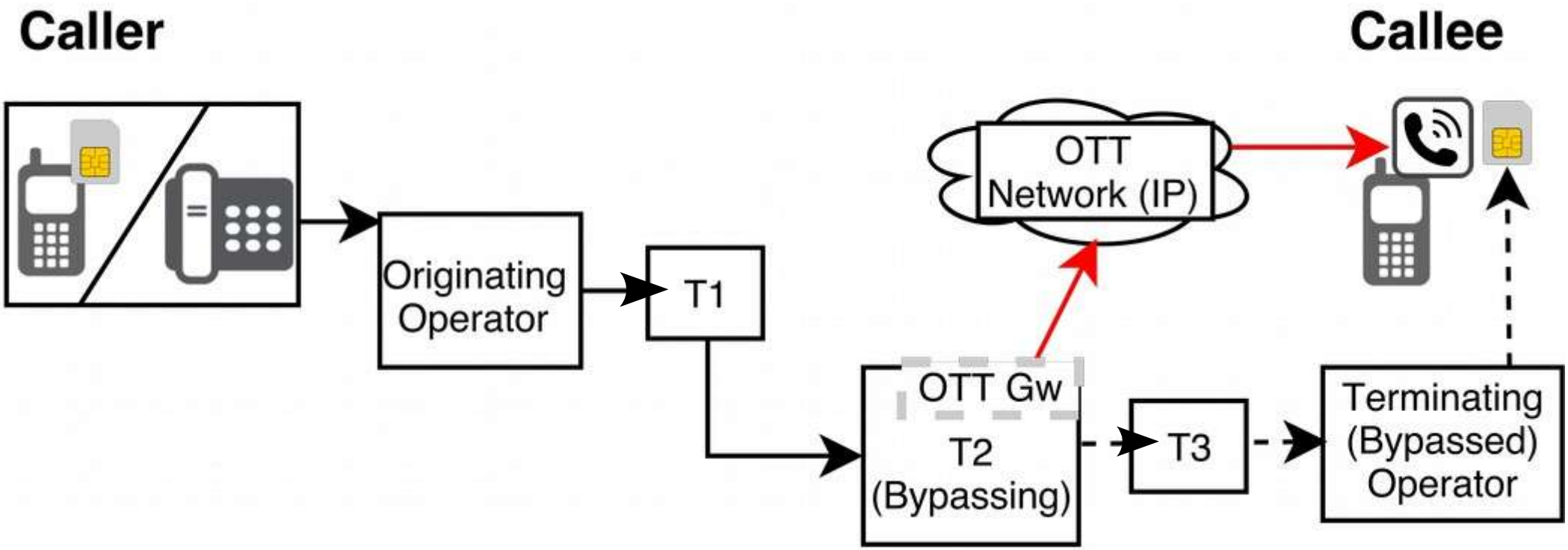


OTT Bypass Call

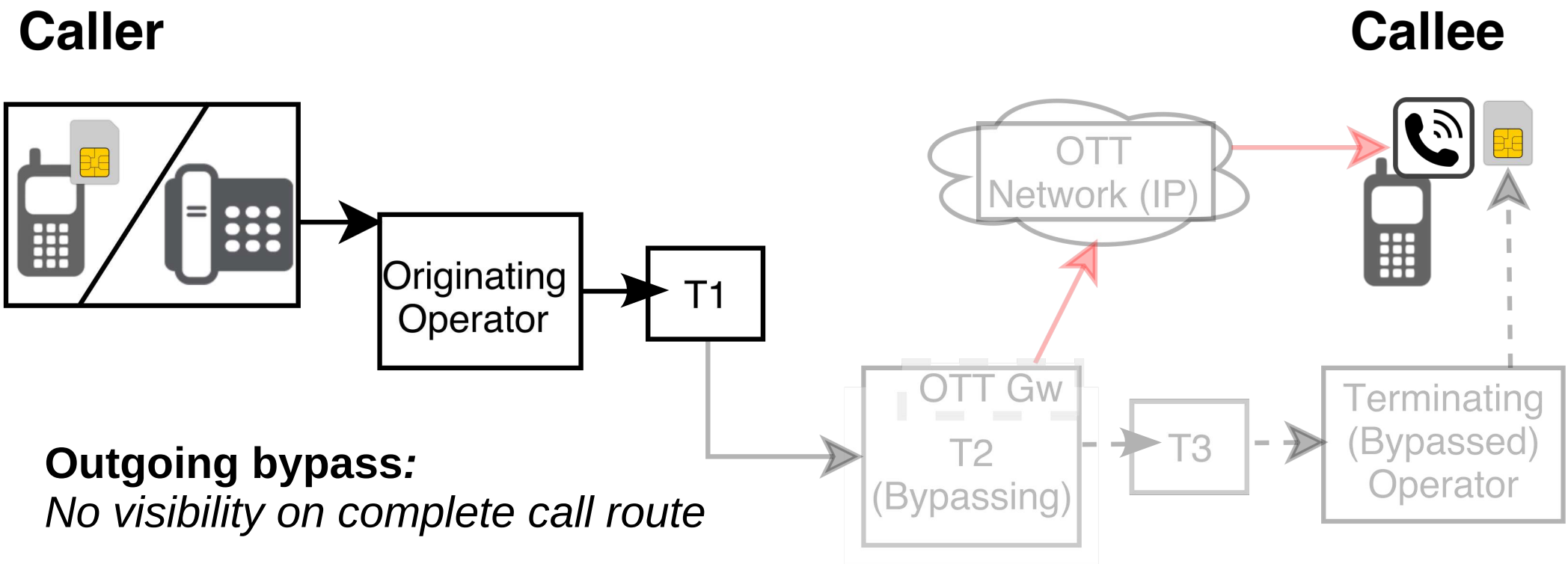


- Significant revenue loss
- Customer dissatisfaction

Detecting and Measuring OTT Bypass: Challenges

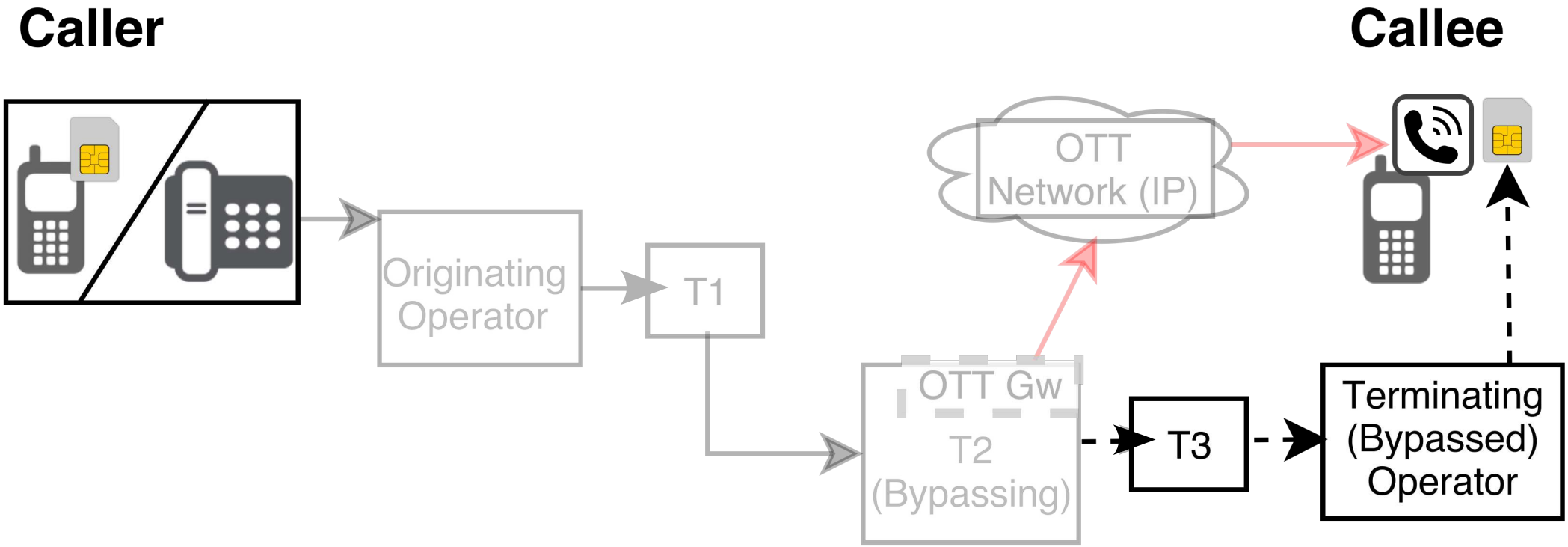


Detecting and Measuring OTT Bypass: Challenges



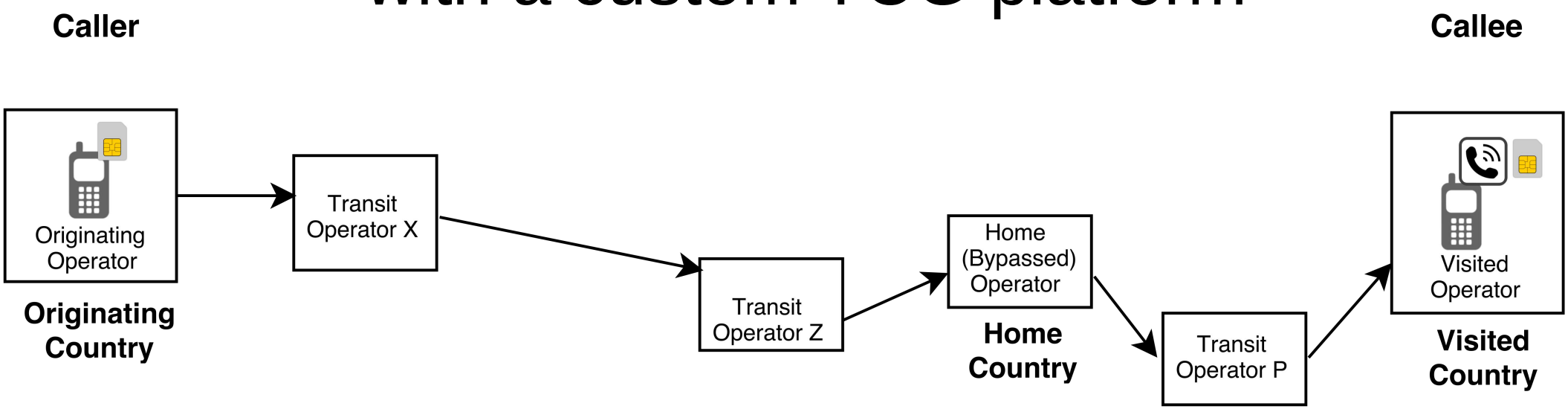
Outgoing bypass*:*
No visibility on complete call route

Detecting and Measuring OTT Bypass: Challenges

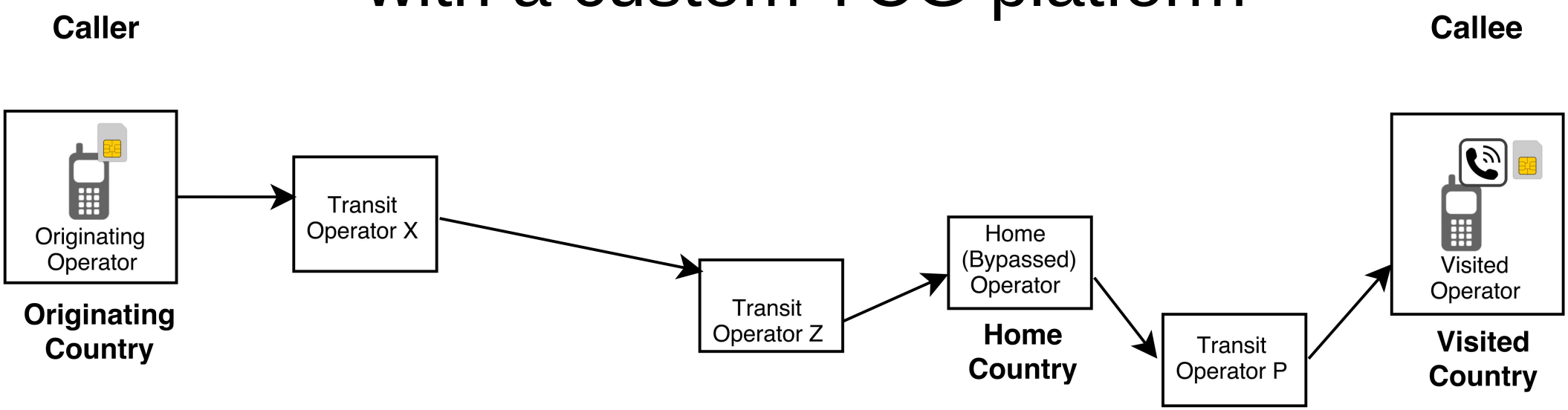


Incoming bypass*:*
No visibility on bypassed call logs

Case Study: Measuring OTT bypass
- on a Small European Country
- with a custom TCG platform



Case Study: Measuring OTT bypass
- on a Small European Country
- with a custom TCG platform



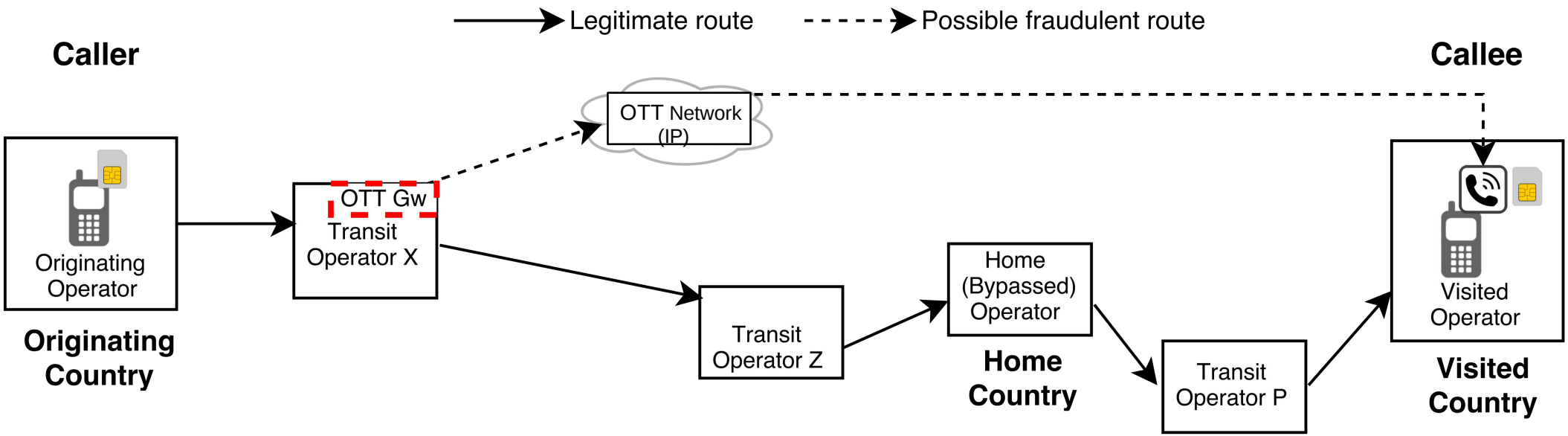
- *Spain*
- *Turkey*
- *United Kingdom*
- *Italy*
- *Netherlands*
- *Germany*
- *Austria*
- *Switzerland*

Experiment Setup

- Customized Android phones
- 4 SIM cards from victim operator
- Recipient phones roaming in France
- Calls originating from 8 countries (1 operator per country)
- Centralized collection of call logs
- 15000 test calls

- *France*

Summary of Results

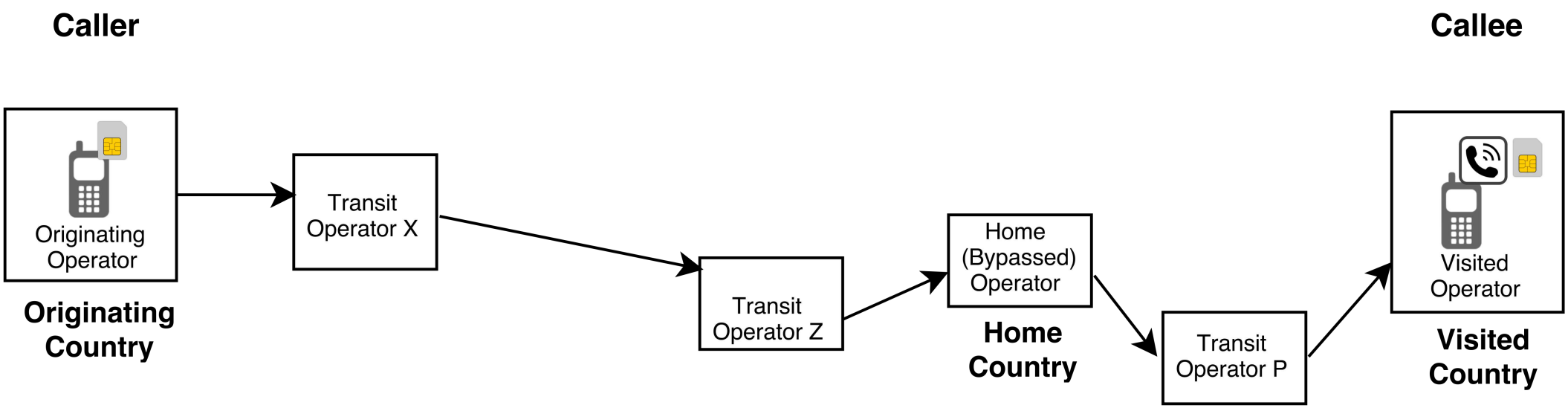


- ***Spain – 83%***
- ***Turkey – 72%***
- ***United Kingdom – 61%***
- ***Italy – 56%***
- ***Netherlands – 53%***
- ***Germany – 42%***
- *Austria*
- *Switzerland*
- *France*

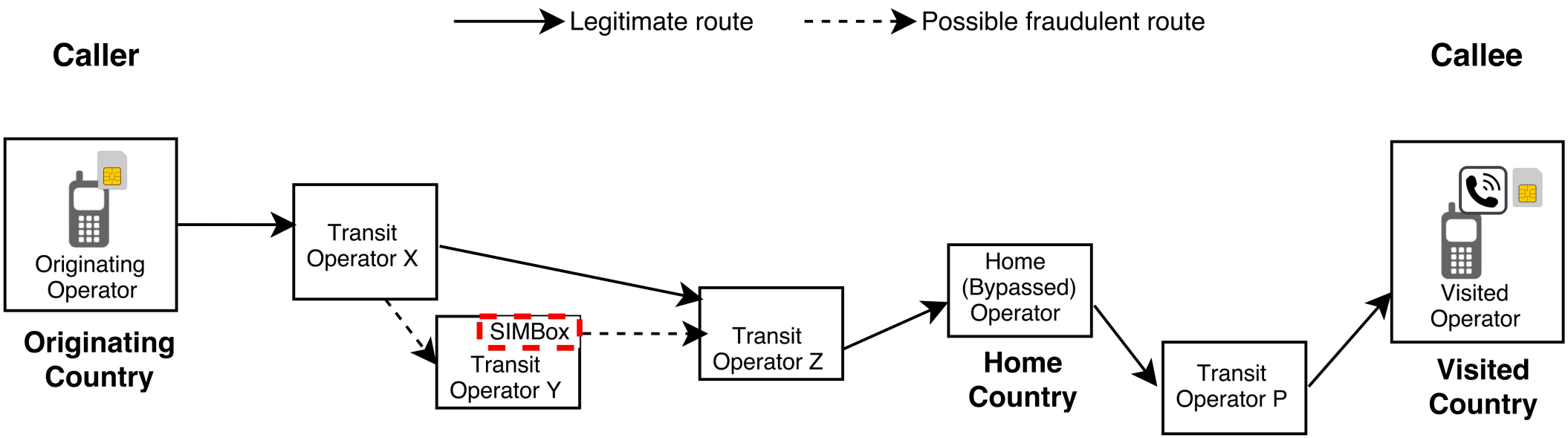
Results

- Up to 83% of calls were subjected to bypass in 6 of 8 countries
- OTT bypass leads to quality problems in call establishment
- Multiple fraud schemes may collide

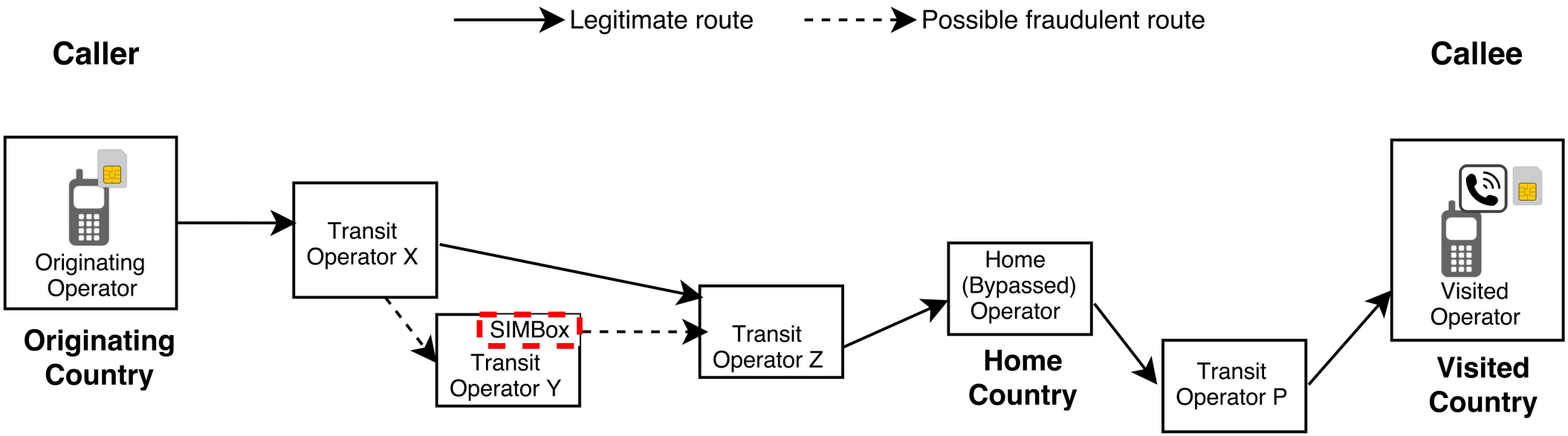
Example: Simbox and OTT Bypass

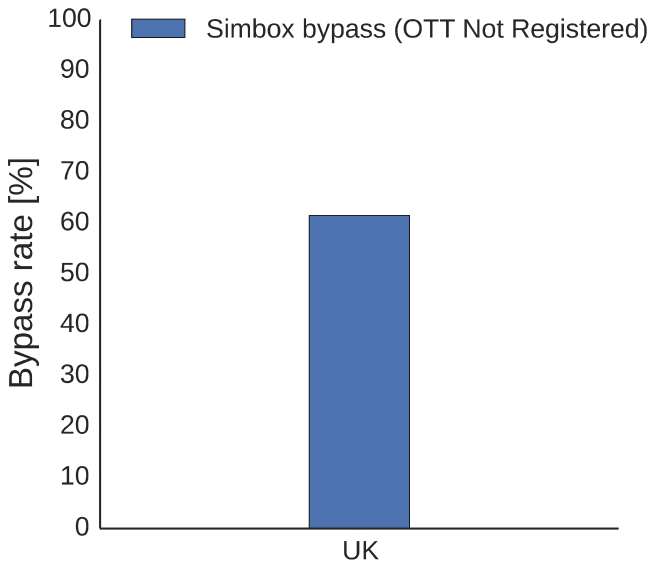


Example: Simbox and OTT Bypass

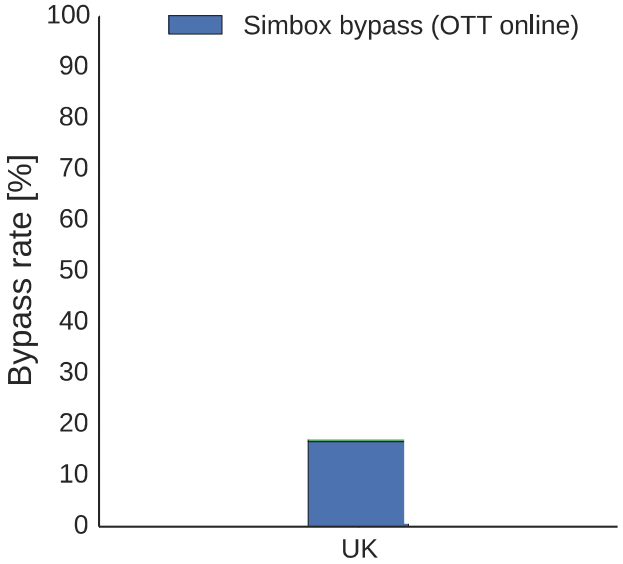


Example: Simbox and OTT Bypass



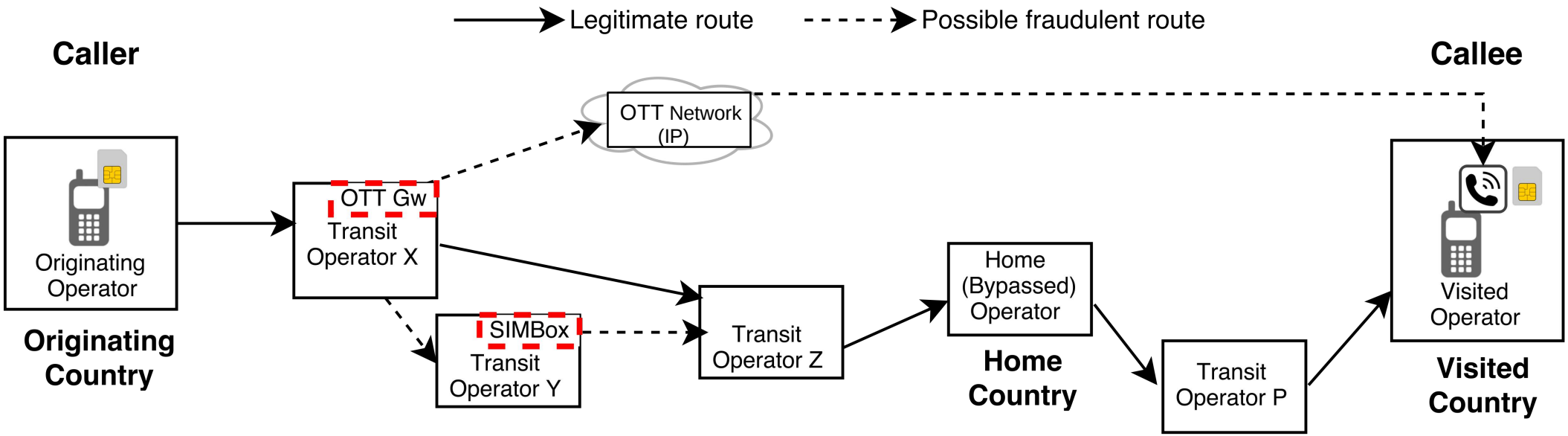


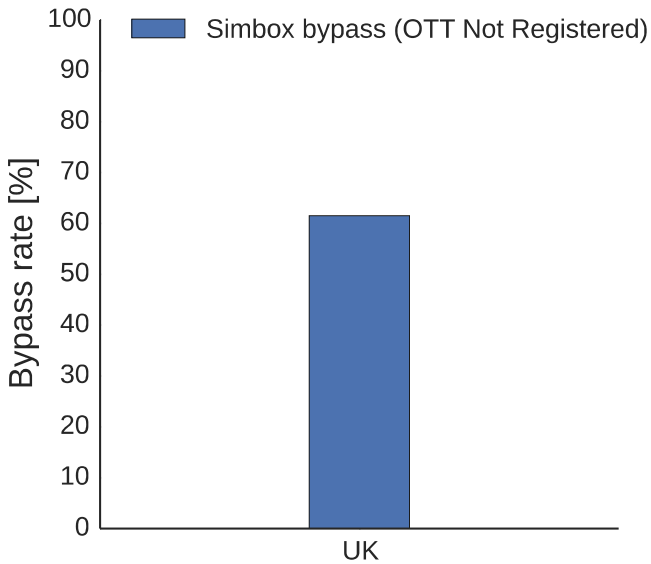
Recipient phone is not registered to OTT



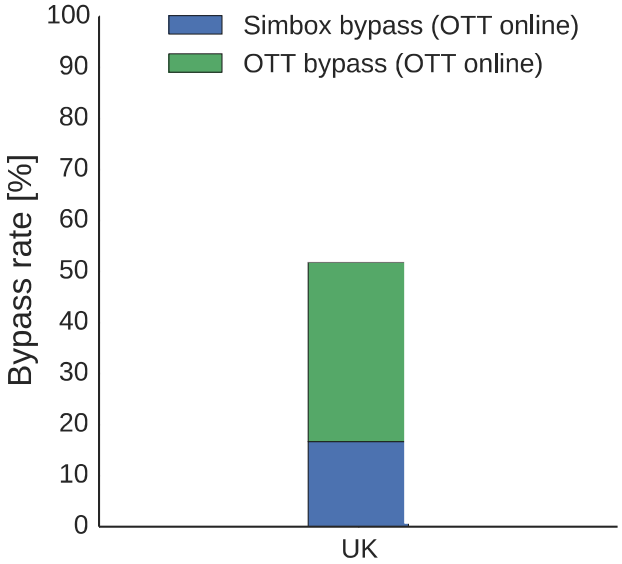
Recipient phone is online on OTT

Example: Simbox and OTT Bypass



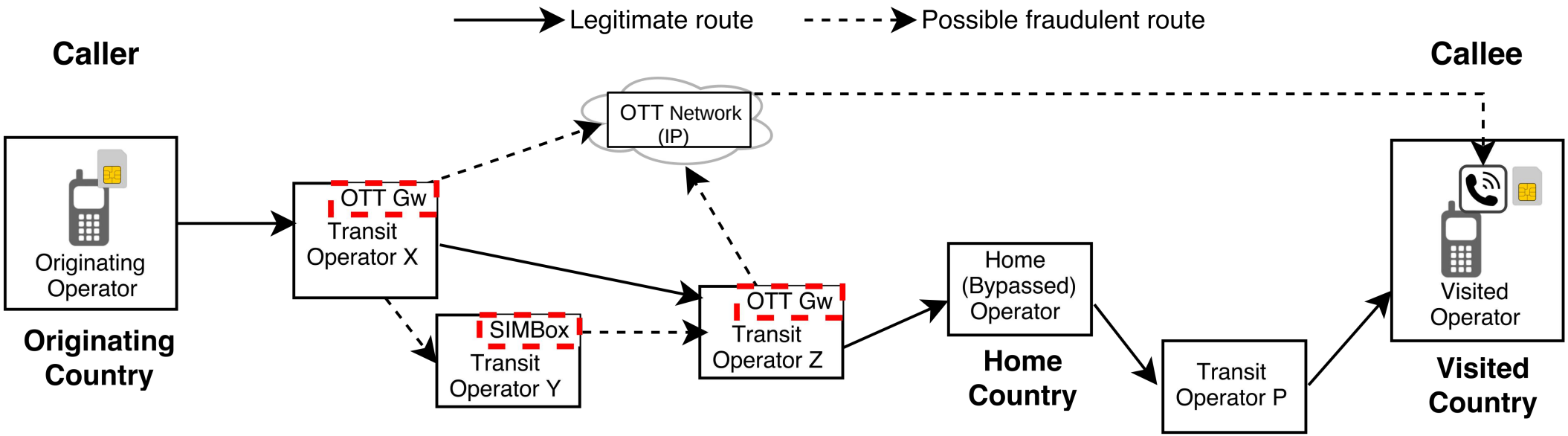


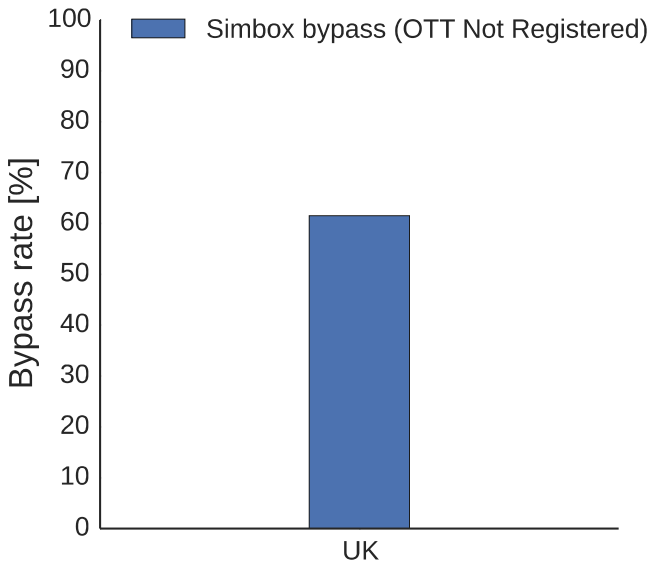
Recipient phone is not registered to OTT



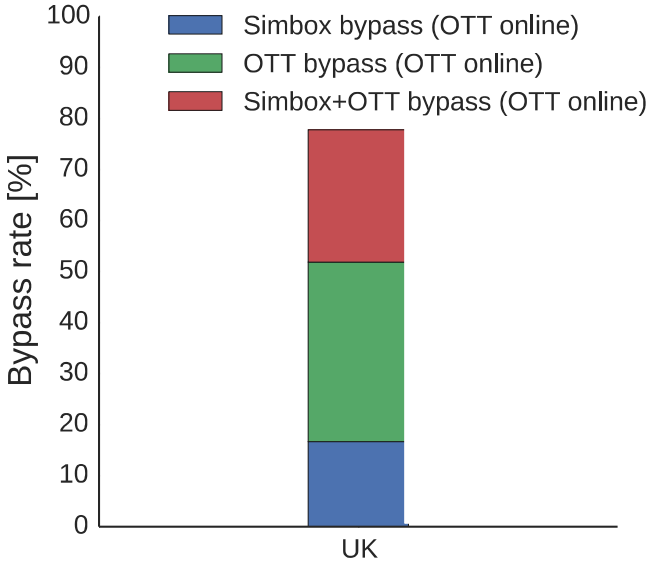
Recipient phone is online on OTT

Example: Simbox and OTT Bypass



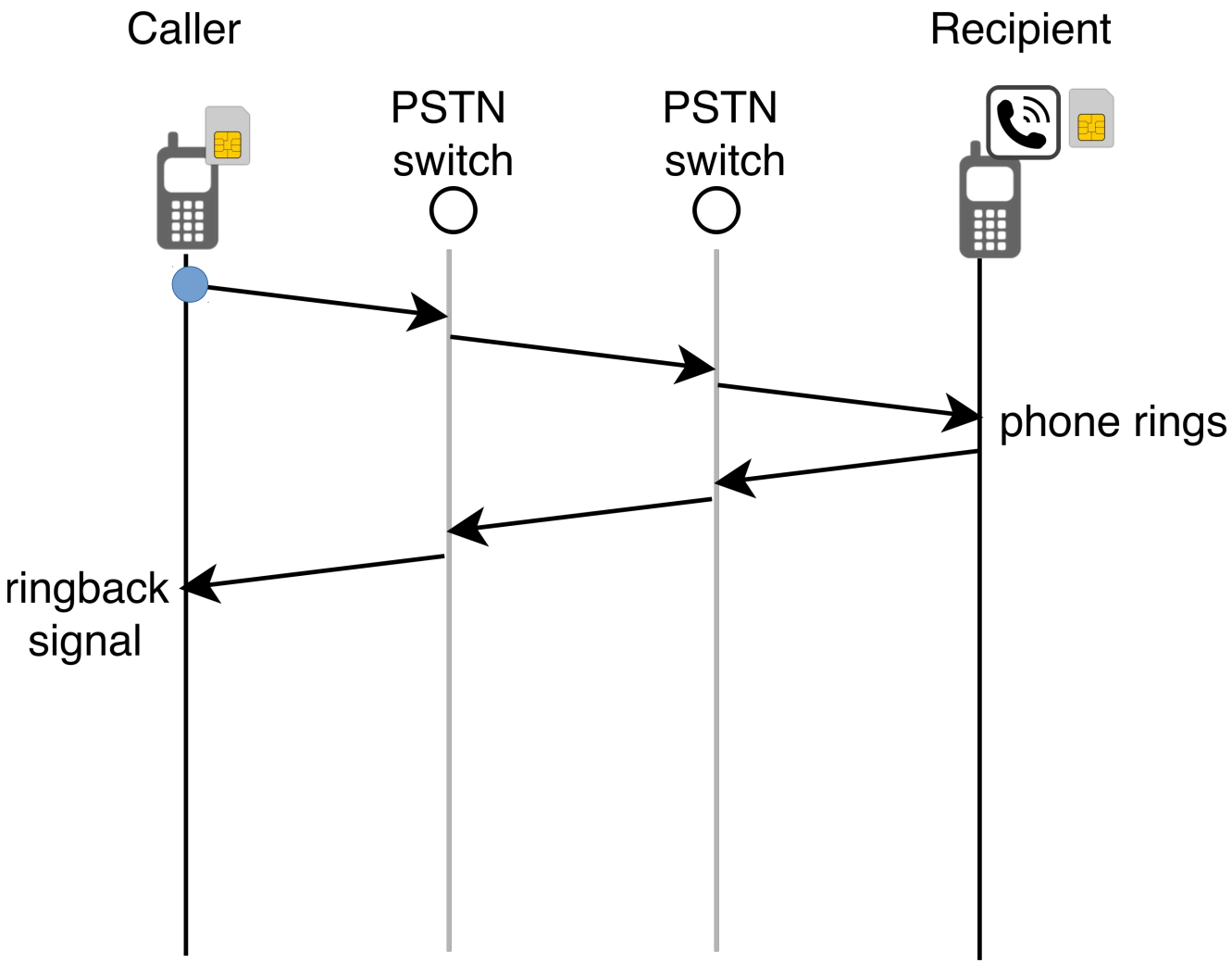


Recipient phone is not registered to OTT

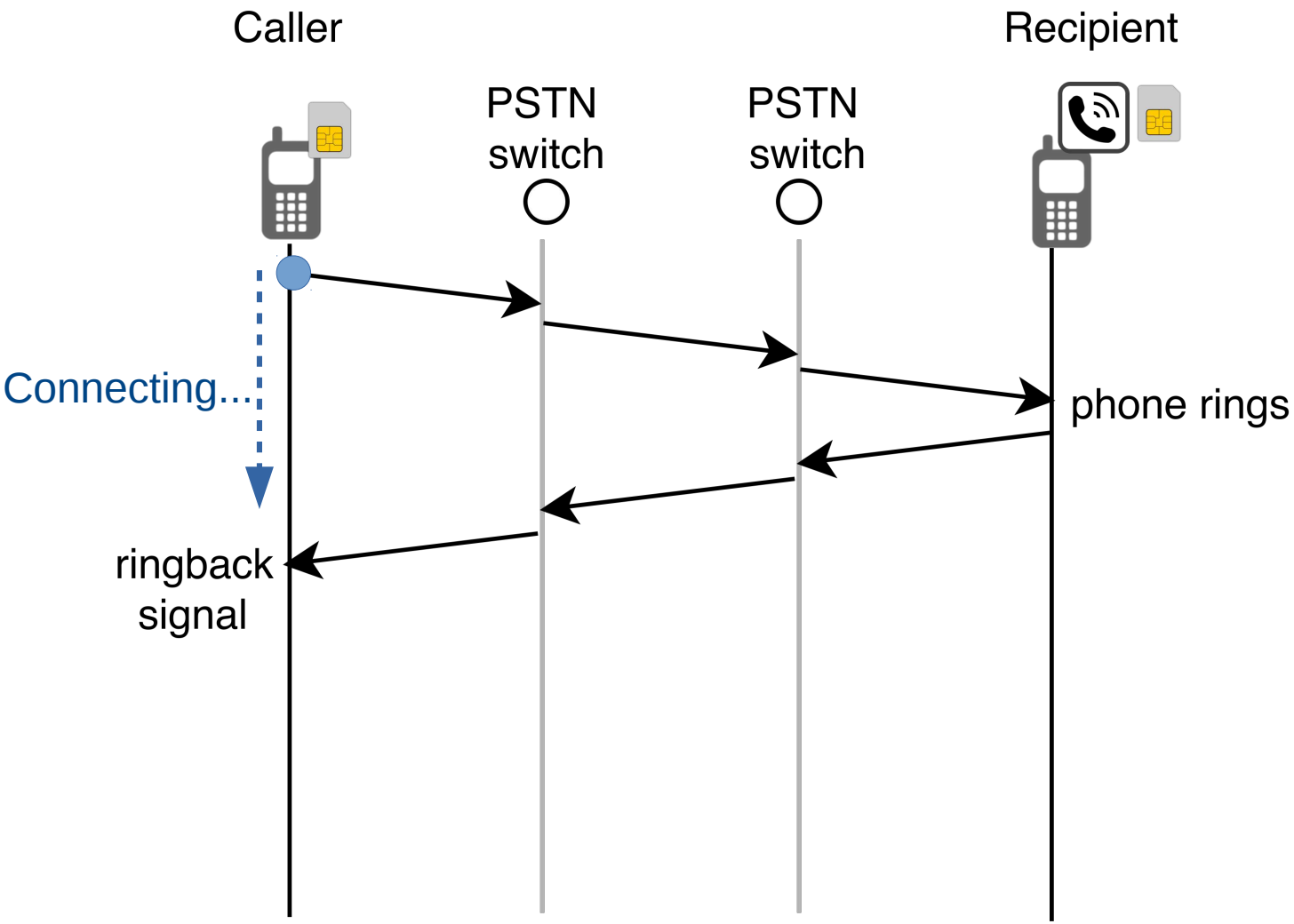


Recipient phone is online on OTT

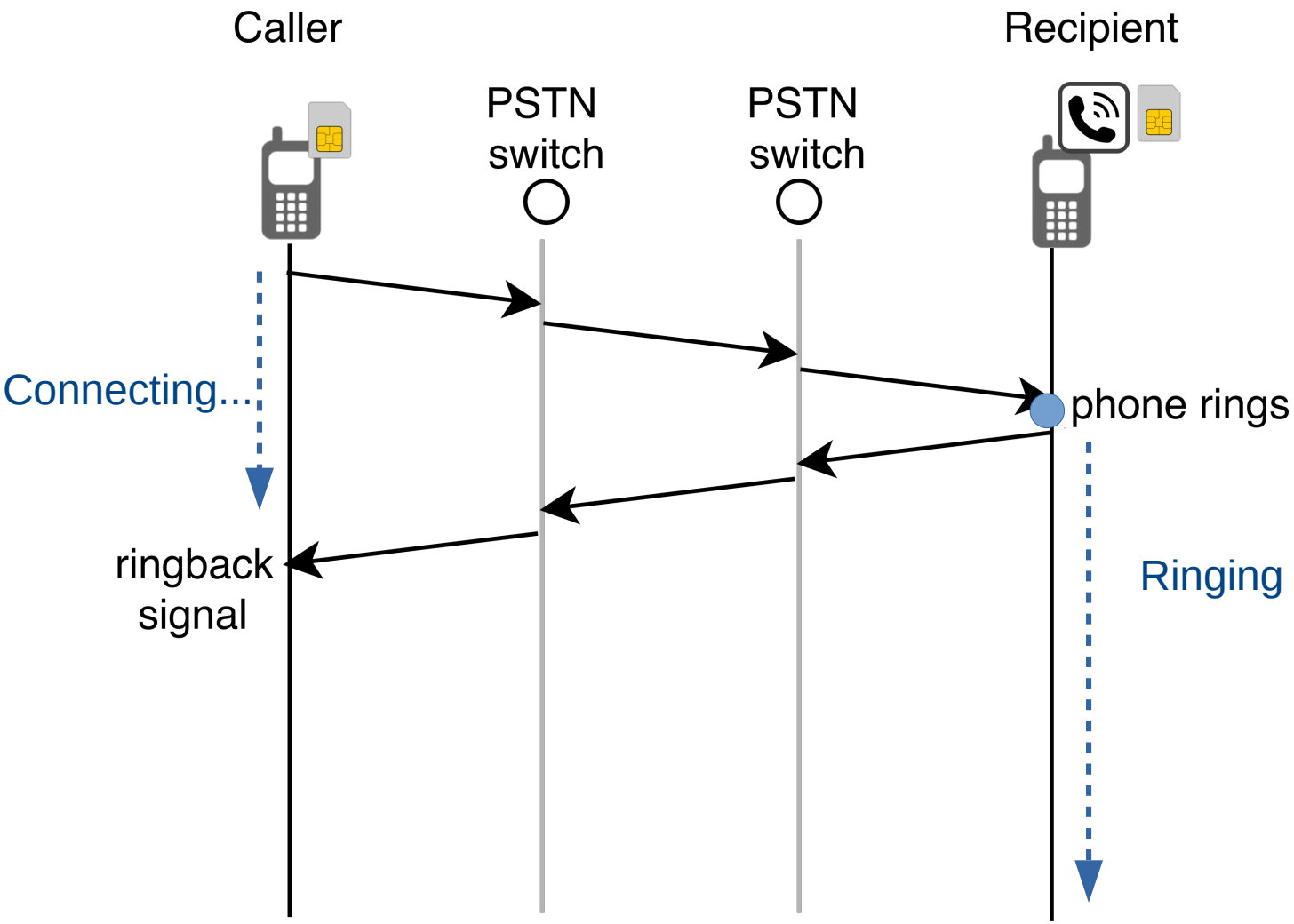
Post Dial Delay (PDD)



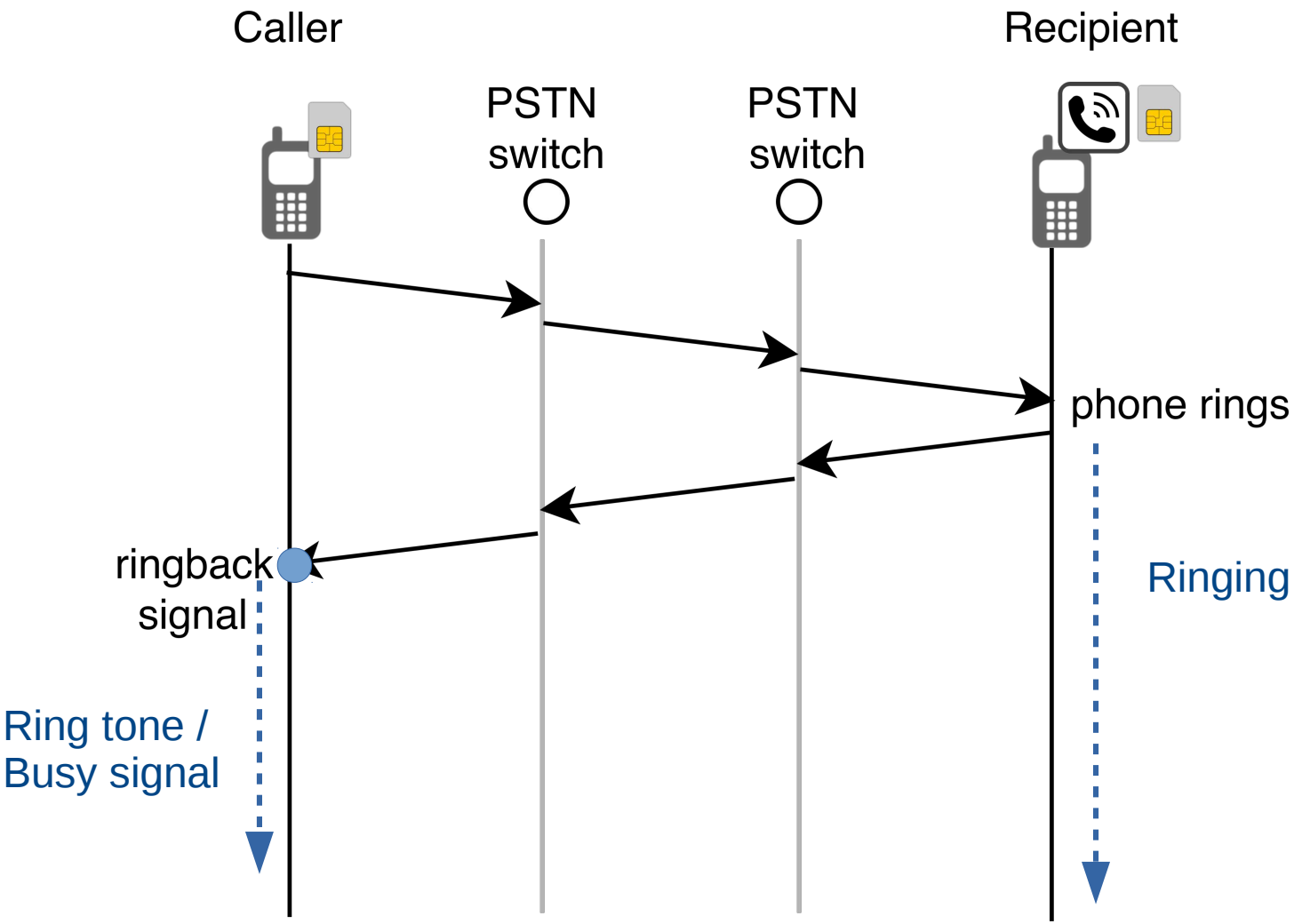
Post Dial Delay (PDD)



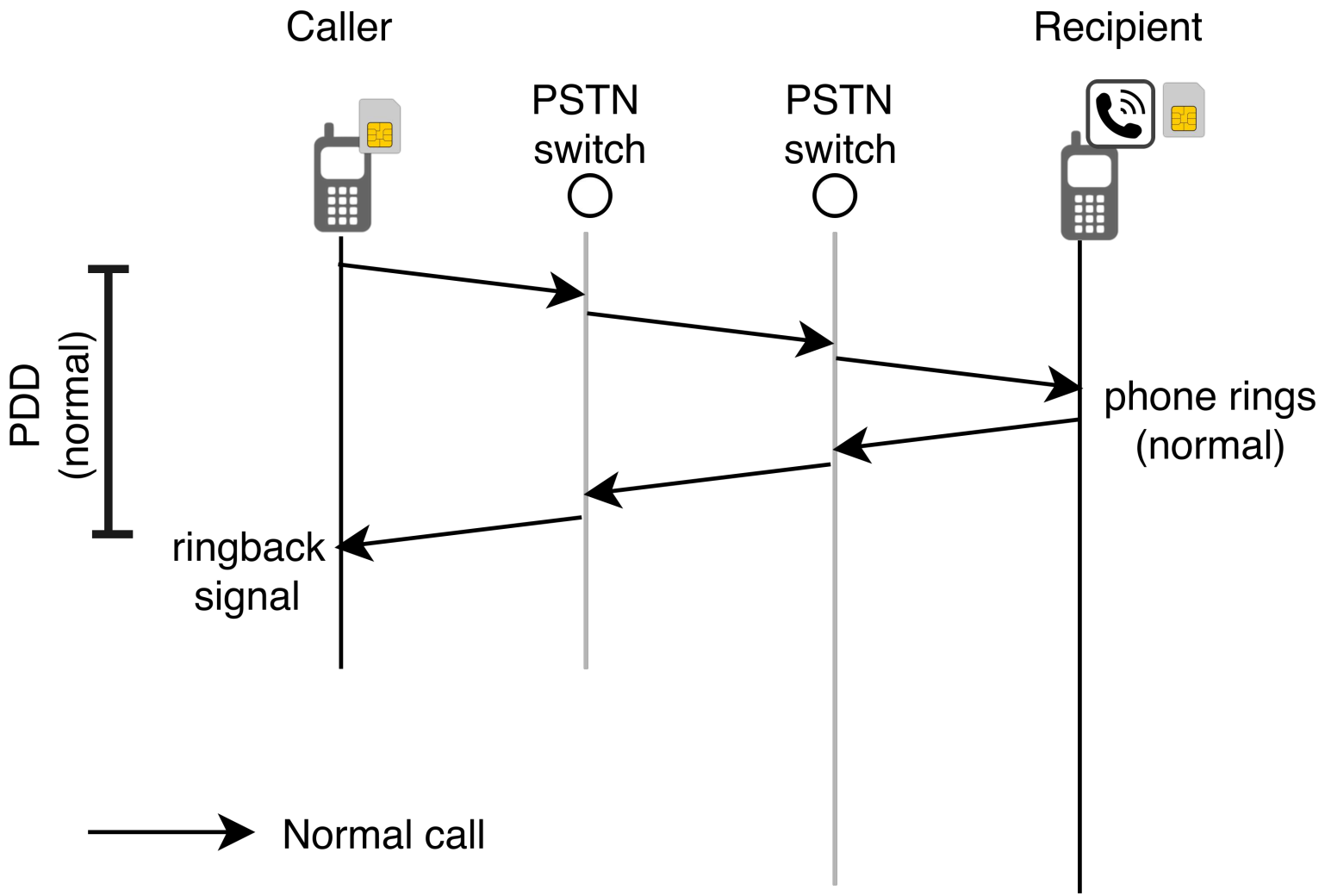
Post Dial Delay (PDD)



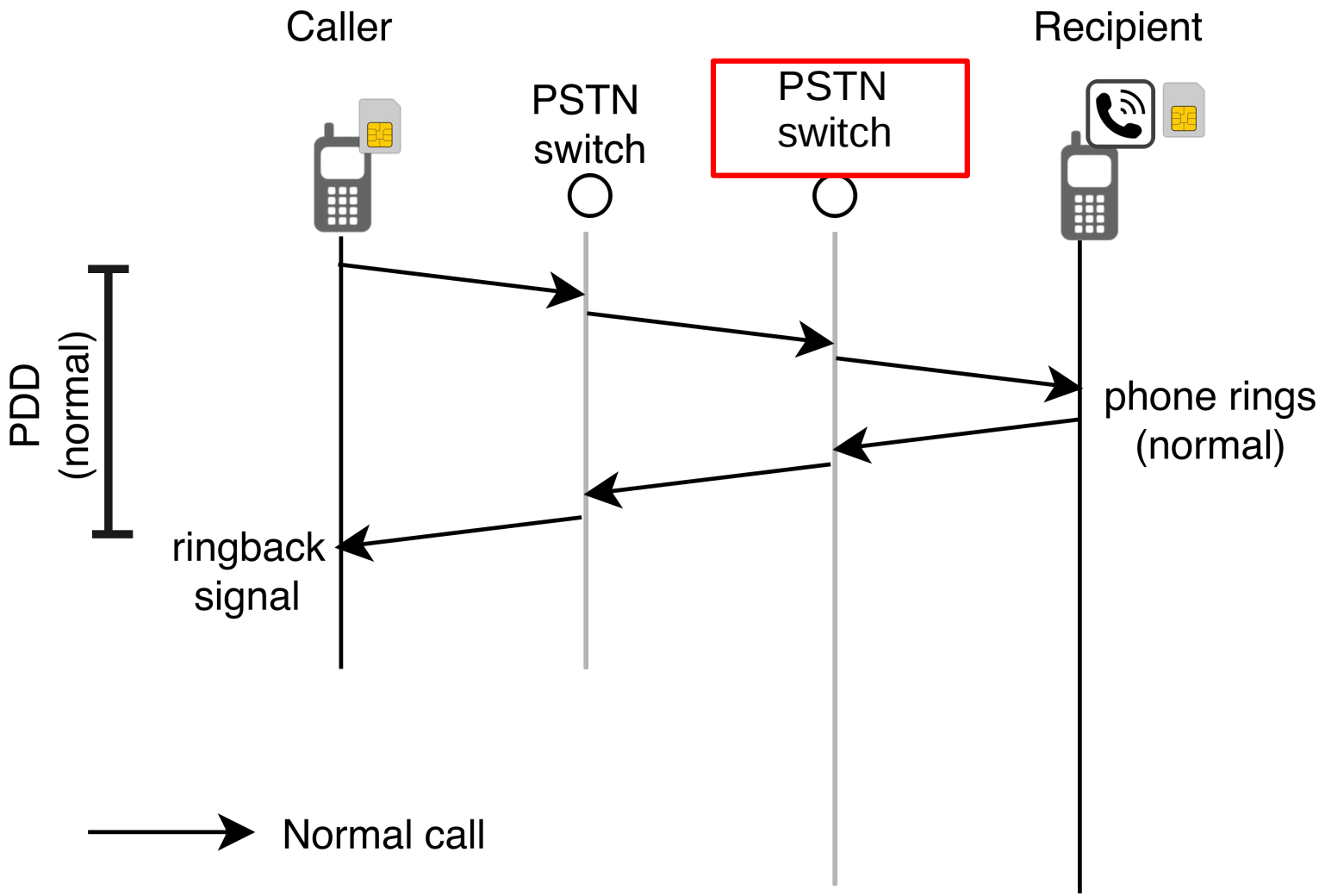
Post Dial Delay (PDD)



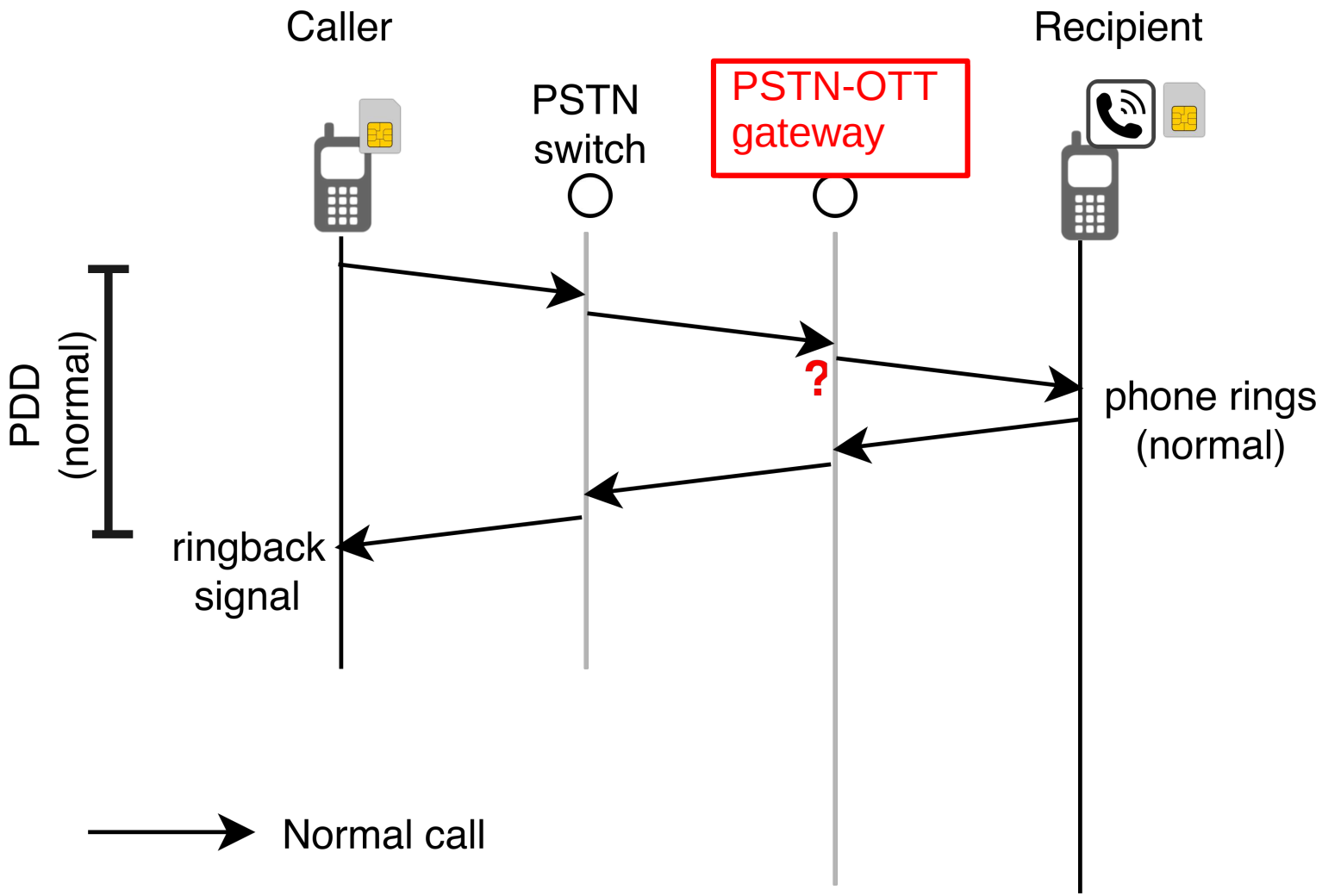
Post Dial Delay (PDD)



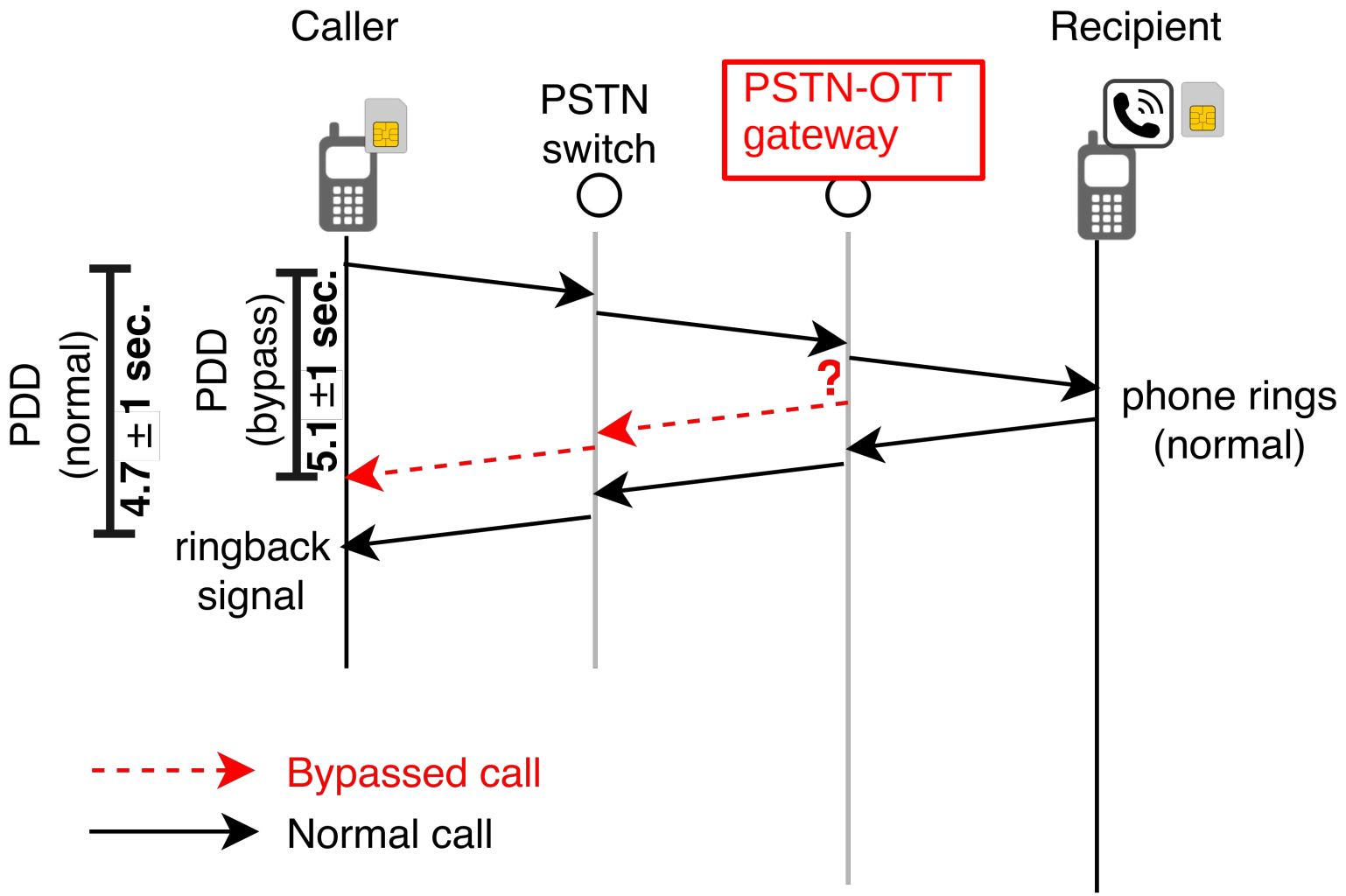
Post Dial Delay (PDD)



Post Dial Delay (PDD)

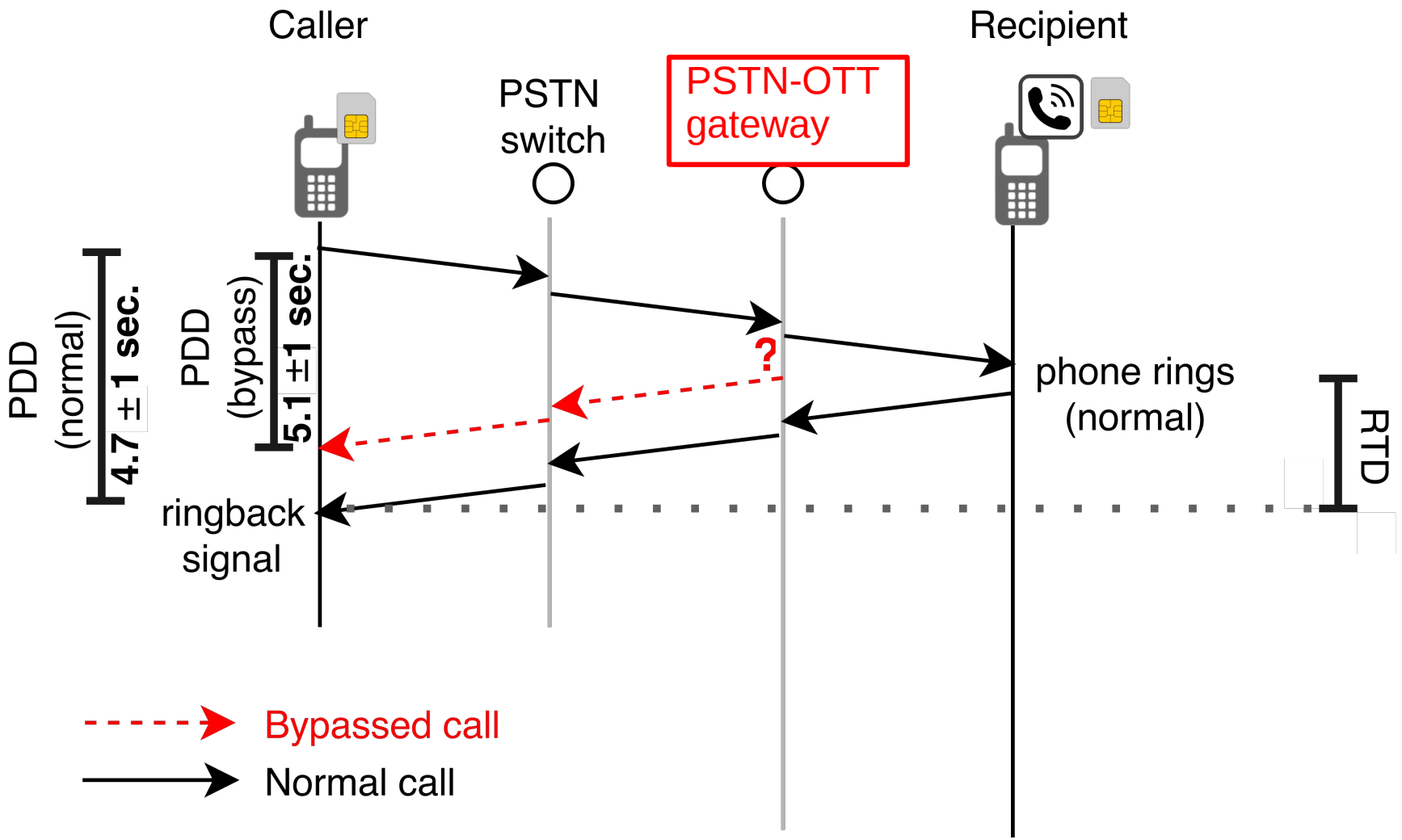


Post Dial Delay (PDD)



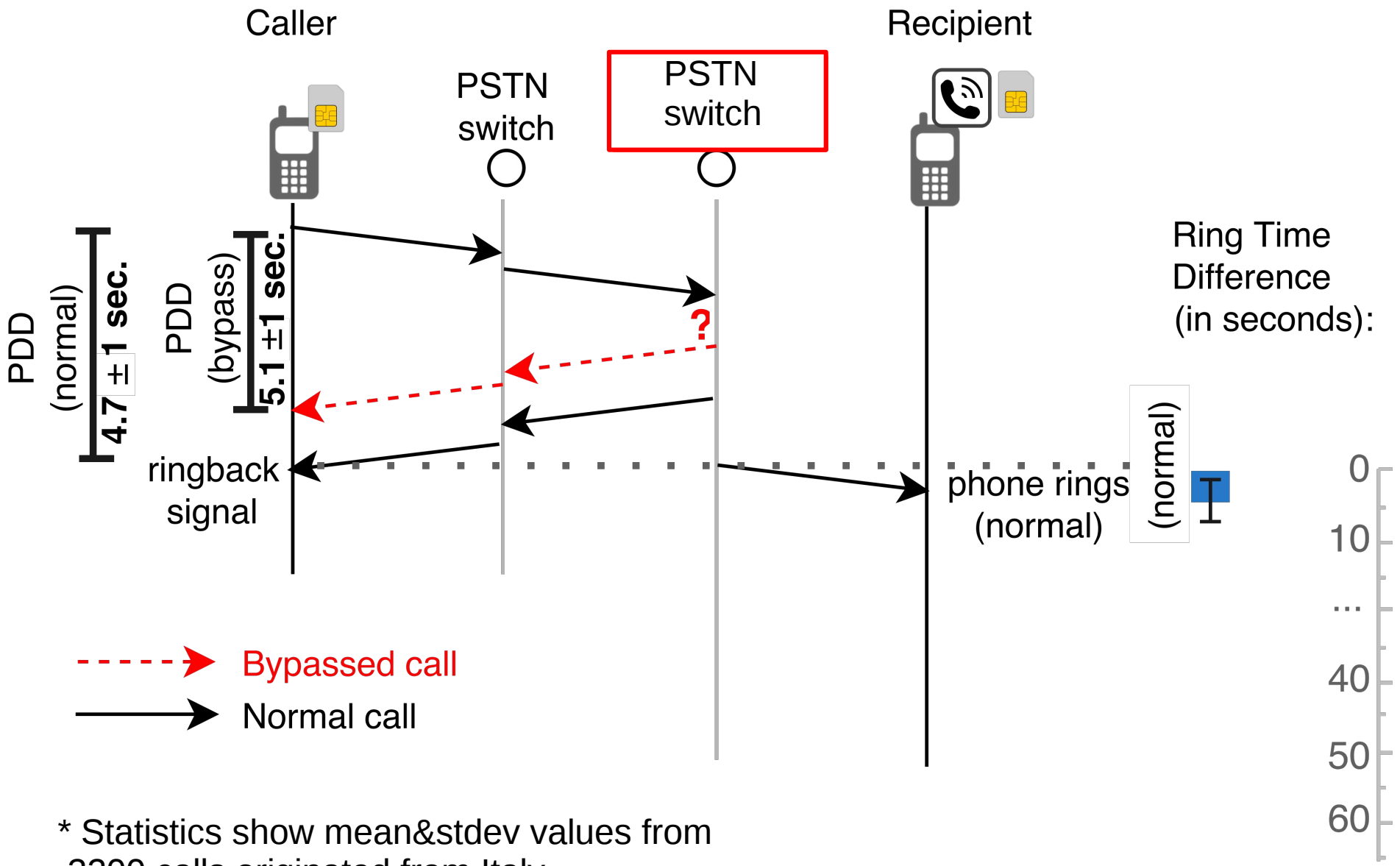
* Statistics show mean&stdev values from 3200 calls originated from Italy.

PDD vs Ring time difference



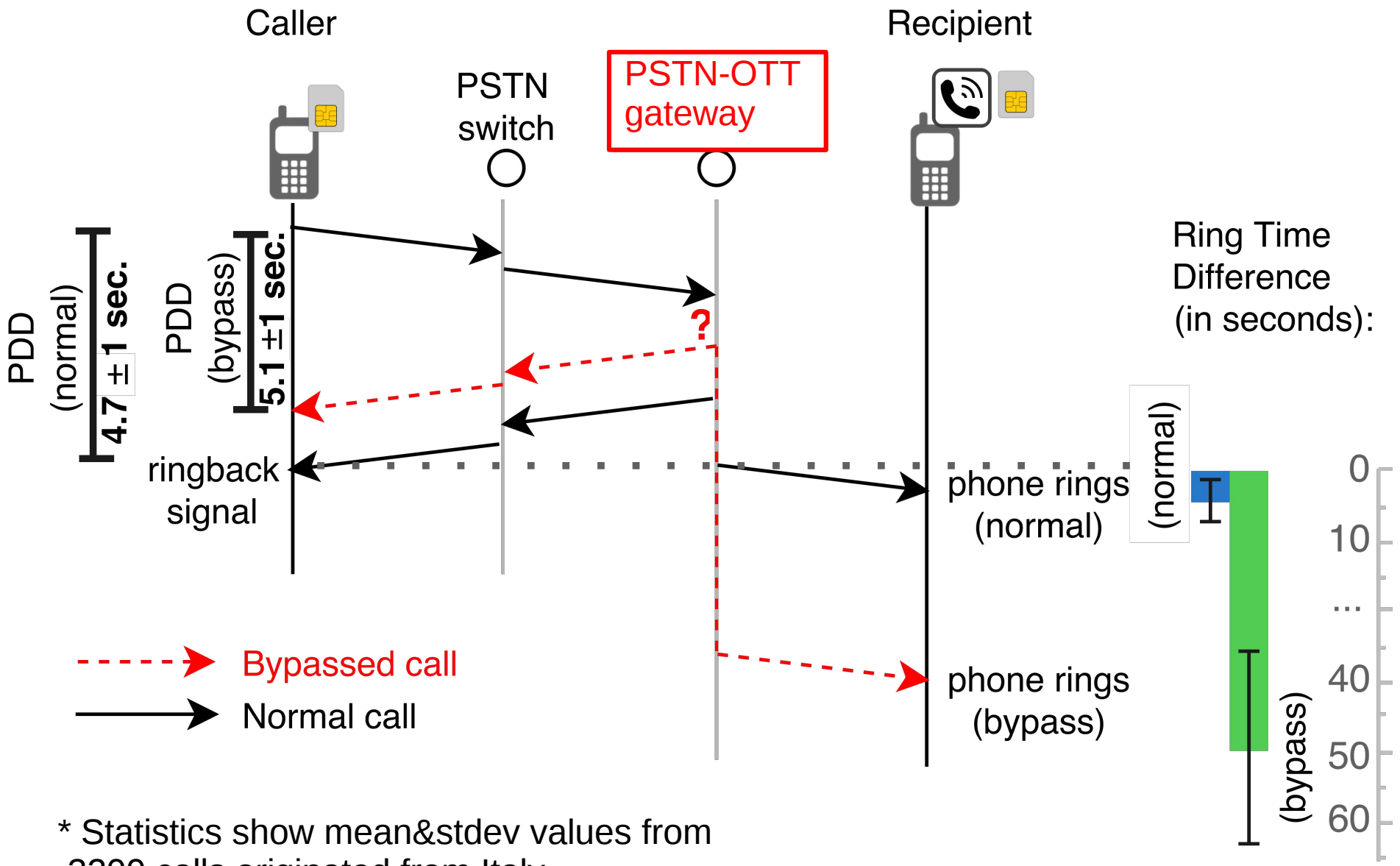
* Statistics show mean&stdev values from 3200 calls originated from Italy.

PDD vs Ring time difference



* Statistics show mean&stdev values from 3200 calls originated from Italy.

PDD vs Ring time difference



* Statistics show mean&stdev values from 3200 calls originated from Italy.

Recap on OTT bypass

- OTT bypass may have severe consequences:
  - Financial losses, customer dissatisfaction for bypassed operators
  - Call establishment problems, unexpected network behavior, SLA violations
  - Poor service quality and no benefits for users
- OTT bypass is challenging to detect and measure
- Blocking OTT / OTT-bypass is a sensitive topic (Network neutrality, freedom of speech)
- Increasing awareness is an important step towards a solution

Conclusions

- Telephony fraud is a complex ecosystem
- A holistic view helps to effectively fight fraud
- Our taxonomy
  - Examines the problem in multiple layers (root causes, weaknesses, techniques...)
  - Helps to better understand
    - Relations and interactions between fraud components
    - Effectiveness and implications of possible countermeasures

Thanks!

References

- M. Kumar, “End of SMS-based 2-Factor Authentication; Yes, It's Insecure!”, 2016. Available at http://thehackernews.com
- V. Prabhu, “How To Hack WhatsApp Using SS7 Flaw”, 2016. Available at https://techworm.net.
- L. Shin, “Hackers Are Hijacking Phone Numbers And Breaking Into Email, Bank Accounts: How To Protect Yourself”, 2016. Available at www.forbes.com.
- L. Shin, “Hackers Have Stolen Millions Of Dollars In Bitcoin -- Using Only Phone Numbers”, 2016. Available at www.forbes.com.
- Miramirkhani et al., “Dial One for Scam: A Large-Scale Analysis of Technical Support Scams”, NDSS'17.
- Guri et al., “9-1-1 DDoS: Attacks, Analysis and Mitigation”, EuroS&P'17.
- D. Cameron, “Major leak exposes 400K recorded telemarketing calls, thousands of credit card numbers”, 2017. Available at www.dailydot.com.
- D. Mikkelson, “Microsoft Impersonation Scam”, 2014. Available at www.snopes.com.
- L. Notenboom, “I got a call from Microsoft and allowed them access to my computer. What do I do now?”, 2014. Available at http://askleo.com.
- K. Hall, “Brit ISP TalkTalk blocks control tool TeamViewer”, 2017. Available at theregister.co.uk
- “Caller ID Revenue Share for Call Centers and Dialers”, 2016. Available at telecombrokers.com.