Intrusion detection mechanisms for VoIP applications

Mohamed Nassar, Radu State and Olivier Festor

LORIA-INRIA Lorraine
France

Outline

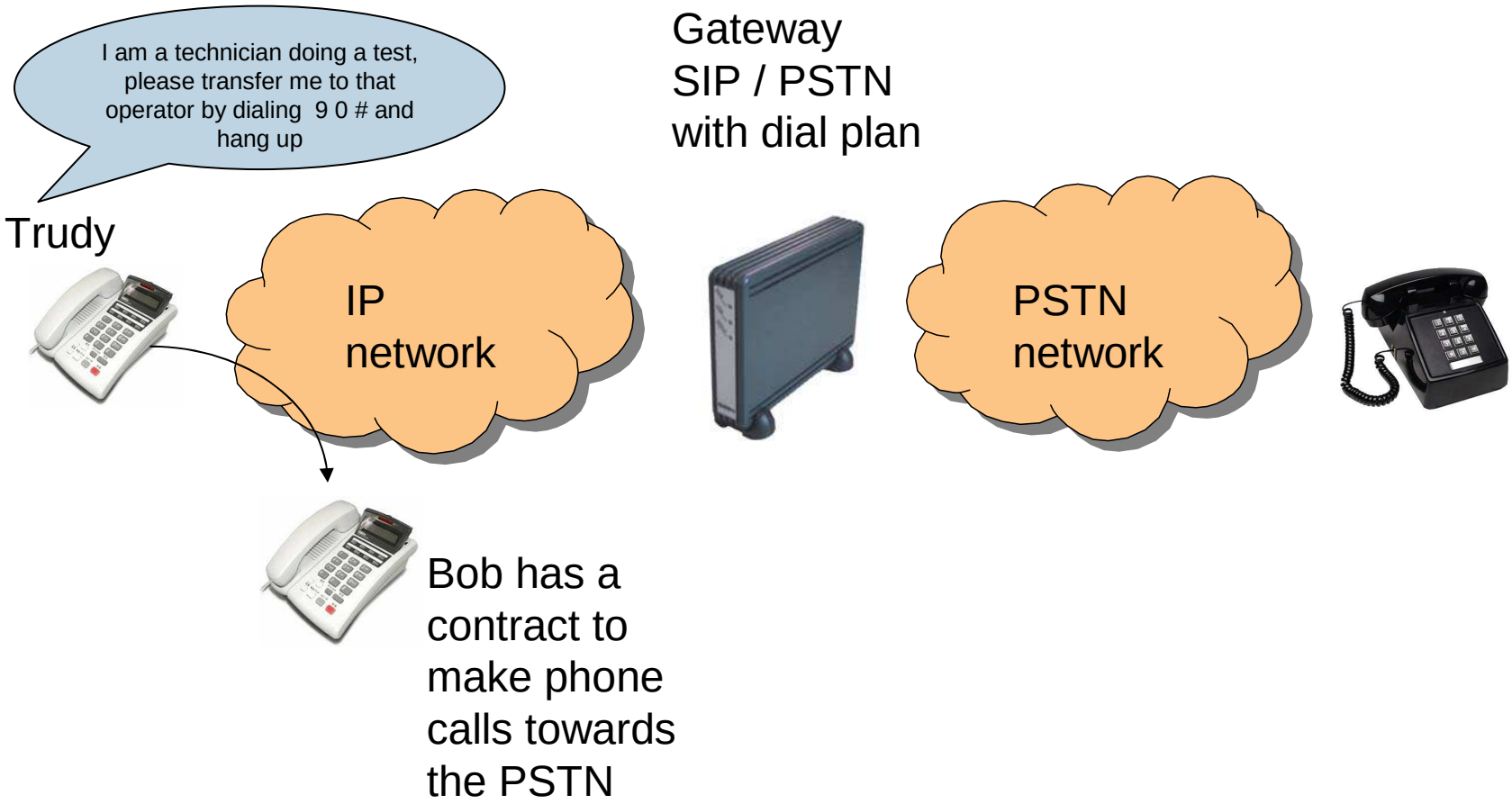
- VoIP Threats
- Objective
- Bayesian inference overview
- Bayesian model for SIP
- CPT tables
- Examples of detection
- Problems
- Futur works

VoIP threats

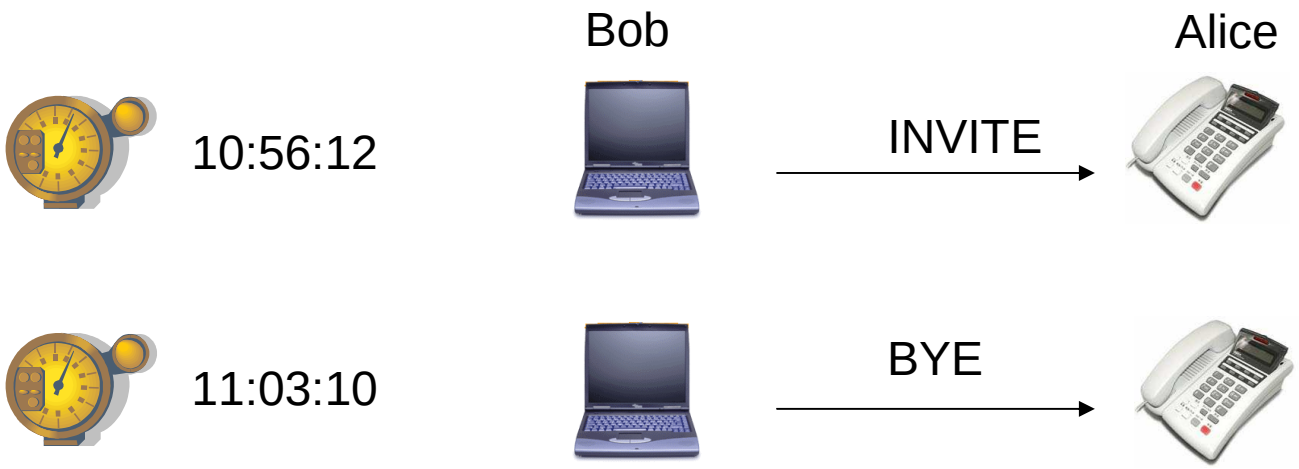
- Social engineering
- Messages interception
- Call tracking
- Phreaking (fraudlent usage)
- Eavesdropping
- Password cracking
- User enumerating
- Call hijacking
- Man in the middle
- DOS
- Gateways and voice mail hosts intrusion
- SPIT
- Media related
- Supporting related
- Firewall traversal

"VoIP Security and Privacy Threat Taxonomy"
http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

Toll fraud by social engineering scheme



Messages interception and call tracking



INVITE sip:Alice@berlin.org SIP/2.0
Via: SIP/2.0/UDP
loria.nancy.org:5060;branch=z9hG4bKfw19b
Max-Forwards: 70
To: Alice <sip:Alice@berlin.org>
From: Bob <sip:Bob@nancy.org>;tag=76341
Call-ID: 123456789@loria.nancy.org
CSeq: 1 INVITE
Subject: How are you?
Contact: <sip:Bob@nancy.org>
Content-Type: application/sdp
Content-Length: 158
v=0
o=Bob 2890844526 2890844526 IN IP4 loria.nancy.org
s=Phone Call
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000

BYE sip:Alice@berlin.org SIP/2.0
Via: SIP/2.0/UDP
loria.nancy.org:5060;branch=z9hG4bK392kf
Max-Forwards: 70
To: Alice <sip:Alice@berlin.org>;tag=76341
From: Bob <sip:Bob@nancy.org>;tag=a53e42
Call-ID: 123456789@loria.nancy.org
CSeq: 1 BYE
Content-Length: 0

User enumerating

Trudy investigates the registrar server to know about existant users.

INVITE sip:1000@berlin.org
INVITE sip:1001@berlin.org
INVITE sip:1003@berlin.org
...

extension	IP address
1234	200.201.202.203
...	...

Registrar server

REGISTER

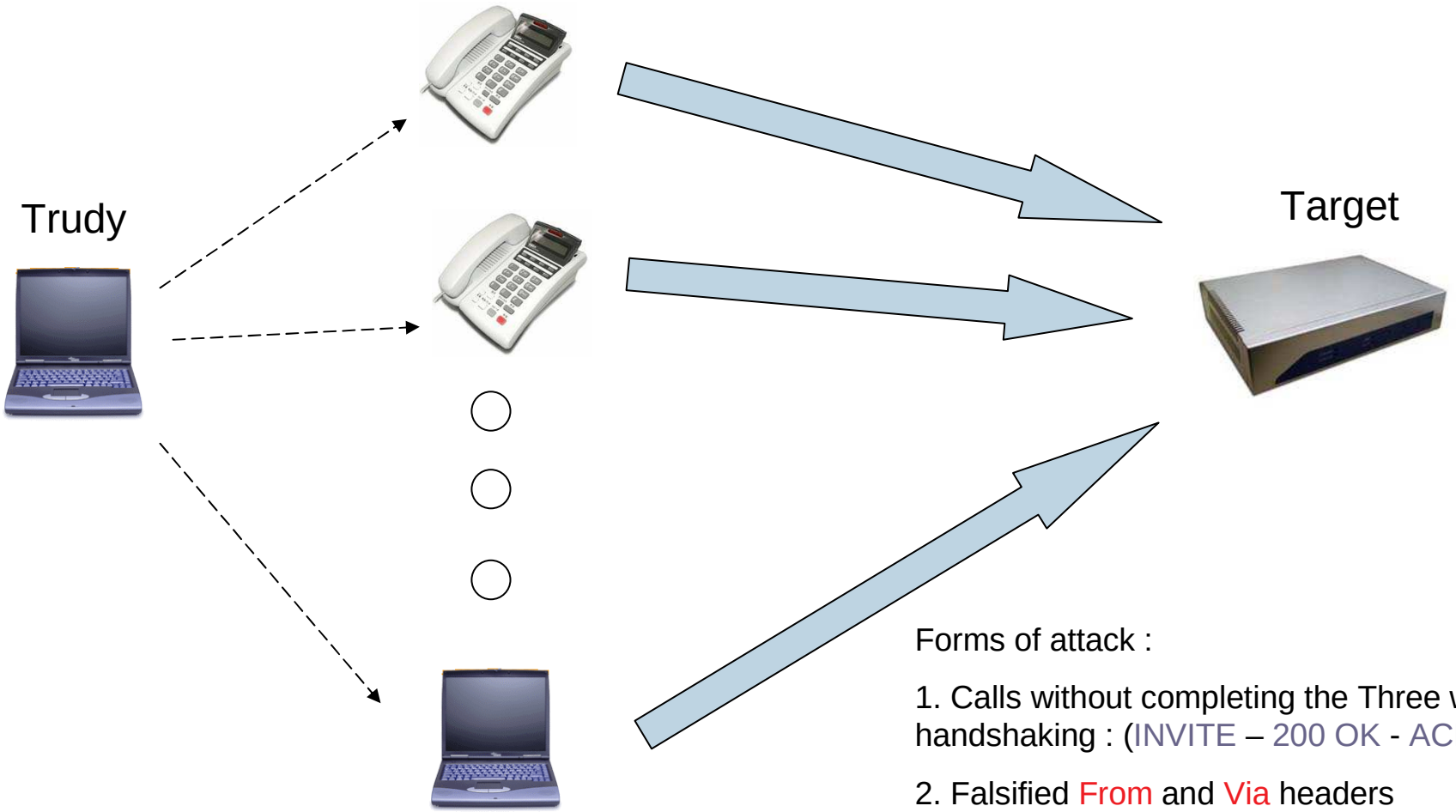
REGISTER sip:registrar.berlin.org SIP/2.0
Via: SIP/2.0/UDP 200.201.202.203:5060;branch=z9hG4bKus19
Max-Forwards: 70
To: Bob <sip:1234@berlin.org>
From: Bob <sip:1234@berlin.org>;tag=3431
Call-ID: 23@200.201.202.203
CSeq: 1 REGISTER
Contact: sip:1234@200.201.202.203
Content-Length: 0

Bob is registered with the extension : 1234

- *User enumerating could be a pre step for SPIT, DOS or Password cracking*

- *User enumerating could take other forms such that assembling numbers from web pages*

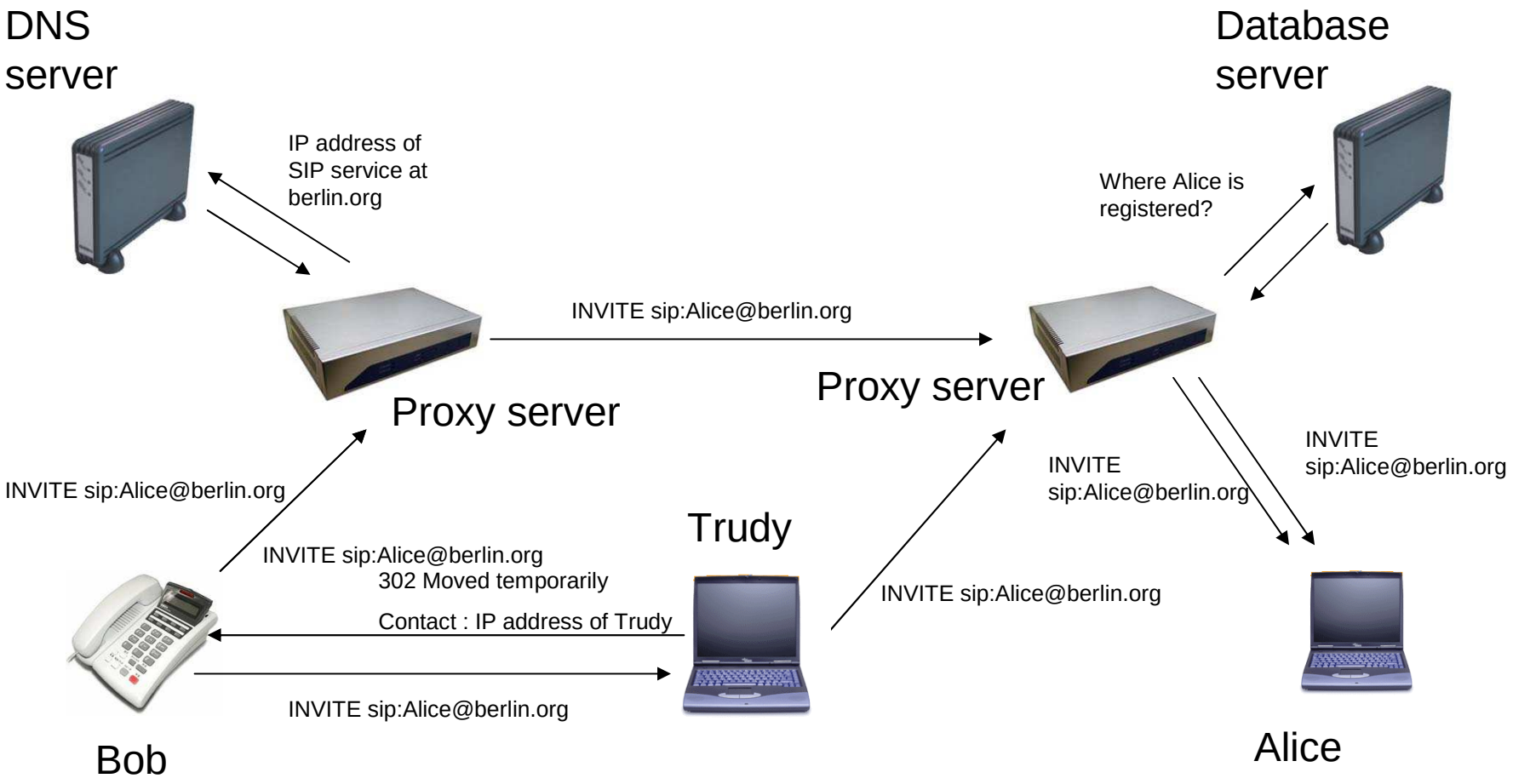
Denial of Service



Forms of attack :

1. Calls without completing the Three way handshaking : (INVITE – 200 OK - ACK)
2. Falsified From and Via headers
3. Using forking proxies with falsified Route header
4. Falsified Record-Route header

Call hijacking and man in the middle



Normal call scenario Attack scenario

Integrated security solutions in SIP

Threat	Solution
Call hijacking and man in the middle	Authentication mechanisms
Eavesdropping	Encryption mechanisms
Tampering the audio or the signaling	Integrity and non repudiation mechanisms

Motivation

- Intrusion detection is a second line of defense behind other security mechanisms (Firewalls, Encryption).
- Supplying the detector engine with application specific knowledge makes it more effective and powerful (lesson from Web based attacks experimenting).
- We were motivated to leverage existing conceptual solutions in intrusion detection for the VoIP specific application domain.
- DOS and SPIT attacks could be the most disturbing attacks with the propagation and deployment of VoIP.
- Bayes model proved a great effectiveness dealing with TCP range of attacks.

Bayesian inference

- Bayesian methods provide a formalism for reasoning about partial belief under conditions of uncertainty

- Formalism :
  - P(H/e): Posterior probability: the belief we accord a hypothesis H upon obtaining evidence e
  - P(e/H) : The likelihood e will materialize if H is true
  - P(H) : Prior probability: previous belief of H
- Empirically verifiable relation ship:

$$P(H/e) = \frac{P(e/H)P(H)}{P(e)}$$

- A Bayesian network:
  - Directed acyclic graph
  - Arrows = causal influences
  - Nodes = random variables

- A Bayesian tree is a Bayesian network where each node might have several children and one parent.

Rules of propagation of belief

CPT = Conditional Probability table

$$CPT_{ij} = P(Child = j / parent = i)$$

π = Prior probability

α = Normalizing constant

$$\pi(Child) = \alpha\pi(Parent) \times CPT(Child / Parent)$$

$\lambda_{to-parent}$ = Influence of one child on the likelihood of the parent

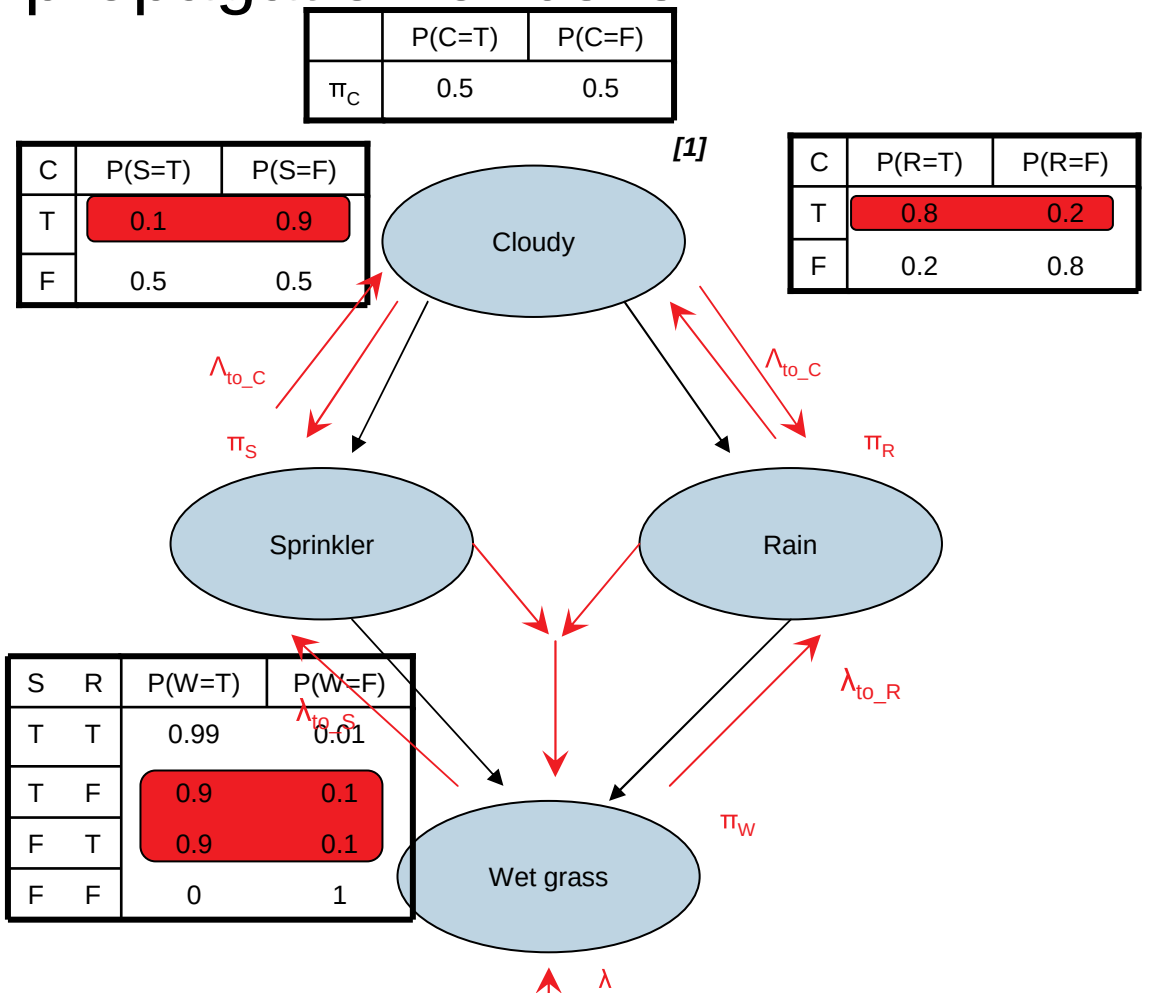
$$\lambda_{to-parent}(Child) = CPT(Child / Parent) \times \lambda(Child)$$

L_i = Elementwise fusion of the likelihood messages at the parent

$$L_i(Parent) = \prod_{Child \in children(parent)} \lambda_{to-parent_i}(Child)$$

BEL_i = The beleif about a class of interest at the root node

$$BEL_i = \beta\pi_i\lambda_i$$



* If the weather is cloudy, so the sprinkler is probably closed
* If the weather is cloudy, so probably it rains
* If the sprinkler is opened or it rains, so probably the grass is wet

[1] **S. Russell and P. Norvig. "Artifcial Intelligence: A Modern Approach." Prentice Hall, Englewood Cliffs, NJ, 1995.**

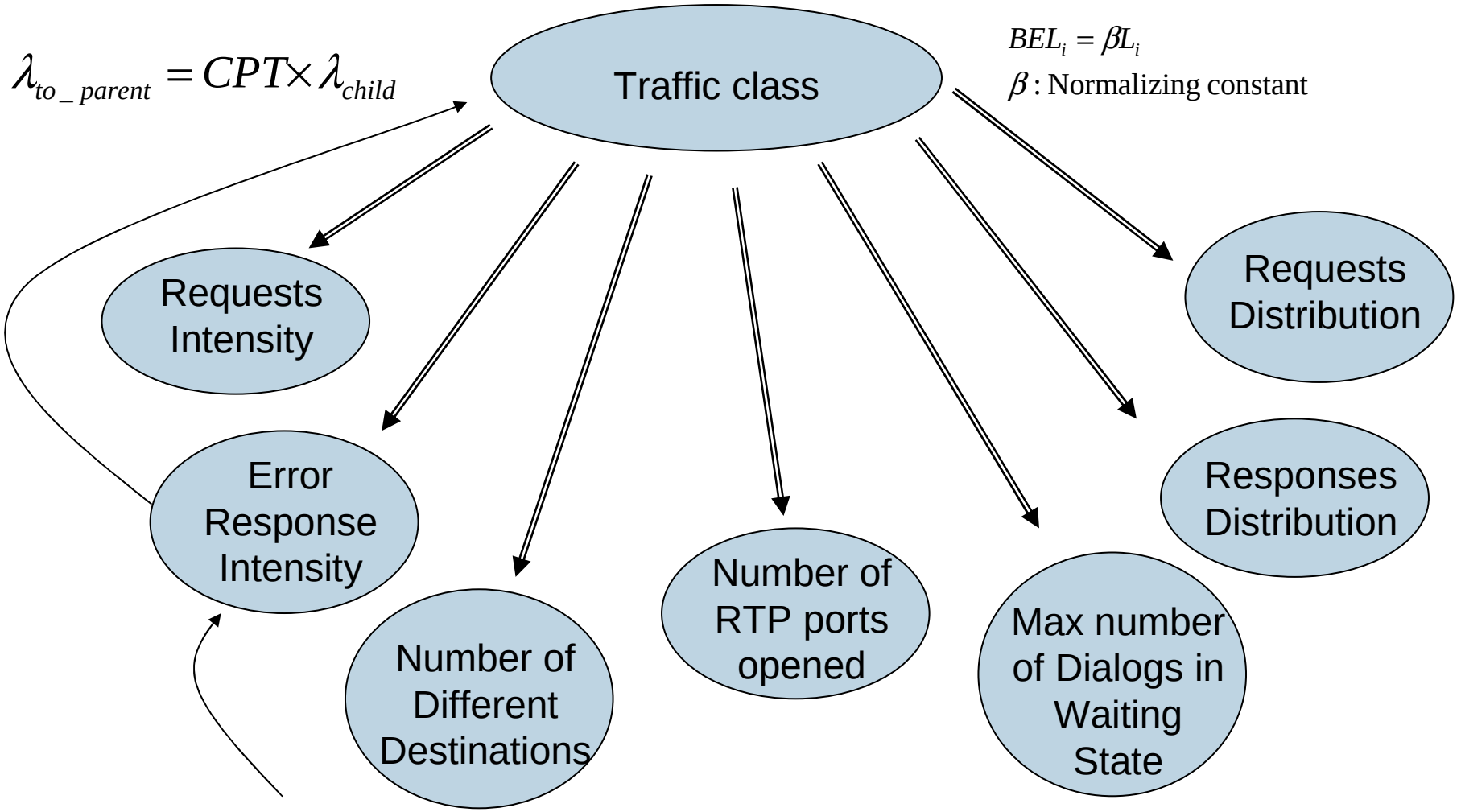
Bayesian model for SIP

$$L_i(Parent) = \prod_{c \in children(Parent)} \lambda_{to\_parent(i)}(c)$$

$$\lambda_{to\_parent} = CPT \times \lambda_{child}$$

$BEL_i = \beta L_i$

β : Normalizing constant



$$\lambda_{Child} = f(observables)$$

Variables definitions

- Intensities
  - Request Intensity : $RI_{req} = e^{k\Delta t}.RI_{req-1} + 1.0$
  - Error Response Intensity : $ERI_{resp} = e^{k\Delta t}.ERI_{resp-1} + I(resp\_code)$
- High Water marks
  - Number of different destinations
  - Number of RTP ports opened
  - Max number of dialogs in waiting states
- Distributions
  - Request distribution: (INVITE REGISTER ACK CANCEL BYE)
  - Response distribution: (1xx 2xx 3xx 4xx 5xx 6xx)

CPT tables

Request Intensity	0-10	>10
Normal	1	0
Scan	1	0
SPIT	1	0
DoS	0	1
Password Cracking	1	0
Firewall Traversal	1	0

Error Response Intensity	0-4	>4
Normal	1	0
Scan	0.2	0.8
SPIT	0.2	0.8
DoS	0	1
Password Cracking	0	1
Firewall Traversal	1	0

Number of opened RTP ports	0-10	>10
Normal	1	0
Scan	1	0
SPIT	0.8	0.2
DoS	0.8	0.2
Password Cracking	1	0
Firewall Traversal	0	1

Number Of Destinations	0-7	>7
Normal	1	0
Scan	0	1
SPIT	0	1
DoS	0.8	0.2
Password Cracking	1	0
Firewall Traversal	0.8	0.2

Max number of Dialogs in waiting state	0-10	>10
Normal	1	0
Scan	0.8	0.2
SPIT	1	0
DoS	0.1	0.9
Password Cracking	0.8	0.2
Firewall Traversal	0.8	0.2

Request	I	R	A	C	B
Normal	0.35	0.10	0.35	0.10	0.10
Scan	0.40	0.05	0.40	0.10	0.05
SPIT	0.40	0.00	0.40	0	0.20
DoS	0.90	0.10	0	0	0
Password Cracking	0.10	0.40	0.40	0.05	0.05
Firewall Traversal	0.40	0.00	0.40	0	0.20

Response class	1xx	2xx	3xx	4xx	5xx	6xx
Normal	0.40	0.40	0.05	0.05	0.05	0.05
Scan	0.10	0.05	0.05	0.70	0.10	0.00
SPIT	0.30	0.20	0.05	0.20	0.20	0.05
DoS	0.20	0.10	0.20	0.20	0.20	0.10
Password Cracking	0.20	0.00	0.10	0.60	0.05	0.05
Firewall Traversal	0.30	0.20	0.05	0.20	0.20	0.05

* In the DoS attack, probably the number of waiting dialogs is higher than 10
* Request is password cracking, surely the request intensity is higher than 4
* In the firewall traversal, the number of SCAN and RTP ports is higher than 10
* In the SPIT and SCAN, surely the number of detinations is higher than 7

Example of detection

Trace of attack

Dialog 1: INVITE → 404 Not Found → ACK

Dialog 2: INVITE → 484 Address Incomplete → ACK

Dialog 3: INVITE → 100 Trying → 503 Service Unavailable → ACK

Dialog 4: INVITE → 100 Trying → 180 Ringing → CANCEL → 200 0K(CANCEL) → 487 Request Terminated → ACK Good number, the attacker hangs up immediately.

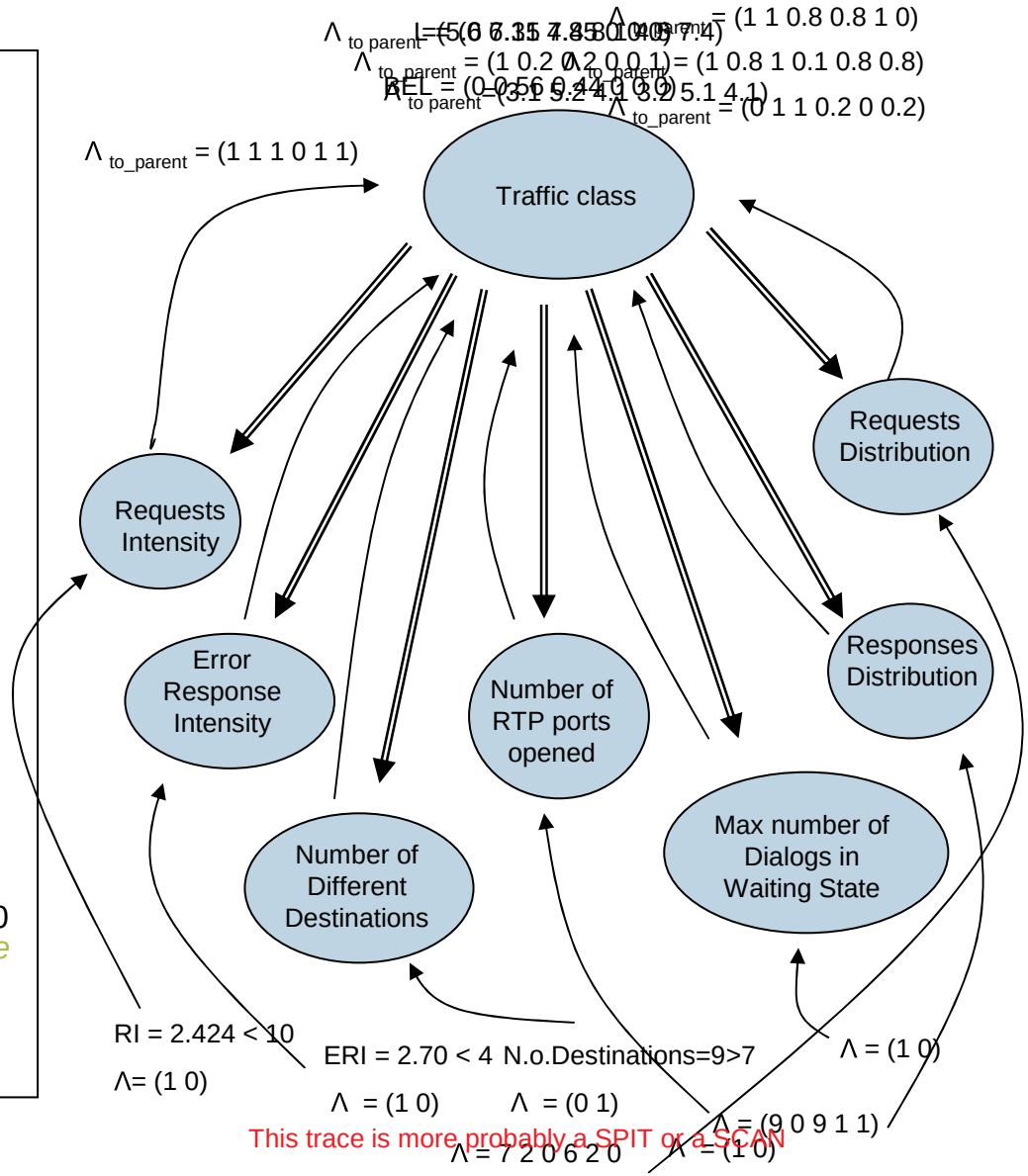
Dialog 5: INVITE → 404 Not Found → ACK

Dialog 6: INVITE → 484 Address Incomplete → ACK

Dialog 7: INVITE → 100 Trying → 503 Service Unavailable → ACK *The number could be right but his owner is not registered at the moment*

Dialog 8: INVITE → 100 Trying → 180 Ringing → 200 OK → ACK → BYE → 200 OK *Good number, the call is answered, the attacker hangs up.*

Dialog 9: INVITE → 404 Not Found → ACK



Problems

- Lack of real world traces for normal and attack kinds of, which is mandatory to :
  - Study the conditional dependency between the observable variables;
  - Set up the CPT tables by a learning phase;
  - Set up the decay rates (thresholds to detect the DoS attacks)
  - Developing the Bayes tree.
- Difficulties in emulating a suitable test bed

(human users of the system)

- We will be happy to find partnerships.

Related works

- Valdez and Skinner used a Bayes tree model to detect a range of TCP attacks [1].
- Service specific anomaly detection proves its efficiency and necessity with Web Based attacks. (Krugel works) [2][3].
- Defense mechanisms to detect SPIT and VoIP specific DoS are discussed in the research community [4][5][6].

[1] *Valdes and K. Skinner. Adaptive, model based monitoring for cyber attack detection. In RAID '00: Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, pages 80–92, London, UK,2000. Springer-Verlag.*

[2] *C. Kr¨ugel, T. Toth, and E. Kirda. Service specific anomaly detection for network intrusion detection. In SAC '02: Proceedings of the 2002 ACM symposium on Applied computing,pages 201–208, New York, NY, USA, 2002. ACM Press.*

[3] *C. Kruegel, G. Vigna, and W. Robertson. A multi-model approach to the detection of web based attacks. Computer Networks, 48(5):717–738, August 2005.*

[4] *D. Shin and C. Shim. Voice spam control with gray leveling. In 2ND Workshop on Securing Voice Over IP. http://www.vopsecurity.org/html/voip security workshop.html 1, Washington, DC, June 2005.*

[5] *Brennen Reynolds and Dipak Ghosal. Secure ip telephony using multi-layered protection. In Proceedings of the Network and Distributed System Security Symposium(NDSS). The Internet Society, 2003.*

[6] *Brennen Reynolds and Dipak Ghosal. Secure ip telephony using multi-layered protection. In Proceedings of the Network and Distributed System Security Symposium(NDSS). The InternetSociety, 2003.*

Future works

- The notion of the Traffic: SIP signaling for a SPIT are events spaced in the time. How could we extract the SPIT traffic ?

Idea : bond graphs (like those used to detect port scans [1])

- Open source VoIP intrusion detection tool covering these and other attacks.

- Real world experiments and real time performance evaluation of our solution.

- Host based solution to defend the new generation of IP PBXs (Asterisk) as well as SIP proxies (SER).

[1] ‘ Practical automated detection of stealthy portscans ’ S. Staniford and J. A. Hoagland and J. M. McAlerney. Journal of Computer Security. Volume 10. Number 1/2. 2002

Questions?

Thank you