MANAGEMENT OF DYNAMIC NETWORKS AND SERVICES

Joint team with Université de Lorraine & CNRS

MADYNES
Nancy – Grand Est
Research Centre

Permanent members & area of expertise

- Laurent Andrey: vulnerability discovery
- Rémi Badonnel: security automation
- Isabelle Chrisment: overlay monitoring
- Laurent Ciarletta: co-simulation & service discovery
- Olivier Festor: monitoring & security automation
- Abdelkader Lahmadi: security automation & vulnerability discovery
- Emmanuel Nataf: Information models, configuration & sensor networks monitoring
- André Schaff: protocol engineering
- *Ye-Qiong Song: Mac layers, cross-layer optimizations, QoS, real-time networks*
- *Thomas Silverston: IPTV, network monitoring*

Applied and Experimental Research in Networks and Services Organization, Management and Security

Managing network vulnerabilities

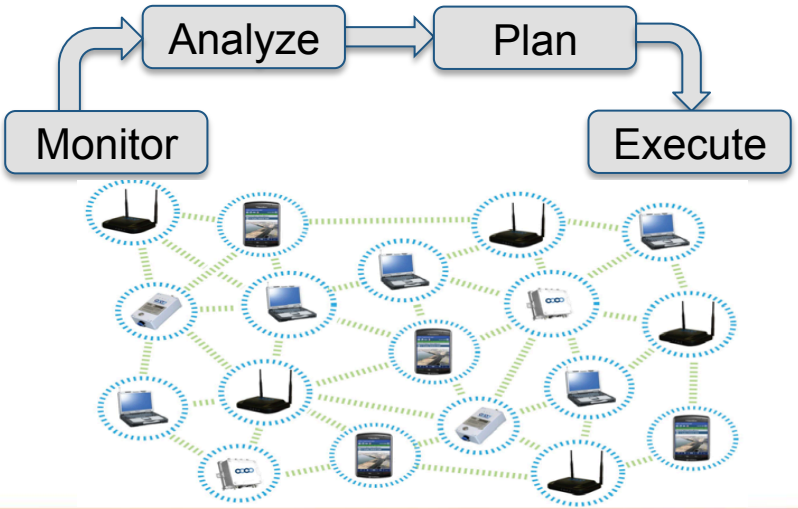
- Discovery
- Exploitation avoidance/mitigation

Detecting malfunction and misuse (monitoring)

- Honeypots, traffic analysis

Improving service and network operation in Smart–spaces

- Co-simulation
- Service discovery



VoIP services
P2P Networks
MANETs
Sensor Networks

Our Value

- 7 successful PhDs & 1 Habilitation degree in the reporting period
- Established & recognized research in Network & Service Management
  - **Leaders of the EMANICS Network of Excellence (2006-2010)**
- Recognized software development & patent
  - **NDPMon (the reference in IPv6 Neigbor Discovery Protocol Monitoring)**,
  - KIF (advanced Fuzzing-based vulnerability detection),
  - Hinky (a collaborative SPIT detection, +40.000 active users)
- Platforms : **High Security Lab** & EMANICSLab
- Joint Team with LIRIMA in Yaounde on Configuration Management
- Established long term external cooperations
  - **CISCO, Alcatel Lucent**
  - 5 FP7 projects including Private Public Partnership
- Strong international activities and high visibility
  - Academics : IEEE TNSM, IJNM, JNSM, CSNM, IM, NOMS, . . .
  - Standardisation : **Chairing the IRTF Network Management Research Group**
  - Organizations : **IFIP TC6, WG 6.6 FIA Future Media Internet task Force, ICT Labs**

Outline

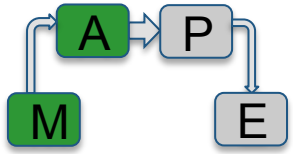
2. Vulnerability discovery
3. Vulnerability exploitation prevention
4. Network monitoring
5. Future work (2012-2015)
6. Summary

2

Vulnerability Discovery

(ALU Joint lab, FIWARE PPP)

Vulnerability Discovery - Challenge



Vulnerability [RFC2828]

A flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's security policy.

Our approach: **Protocol Fuzzing**

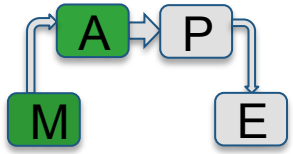
- Large generation & injection of invalid, random or unexpected messages
- 10+ fuzzers in the academic scene and on the market
- **Only ours does stateful fuzzing (e.g. session mgmt):** KIF *[RAID 2008]*

Additional addressed challenges

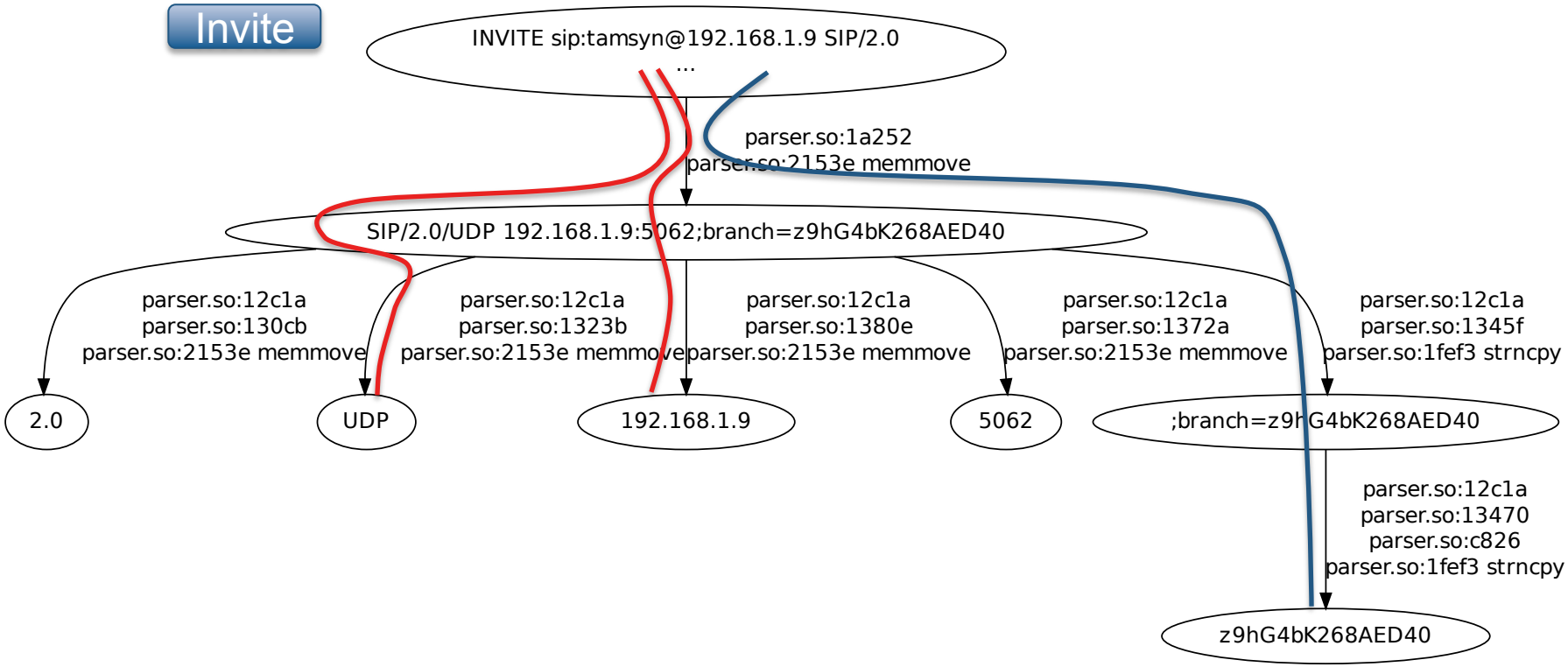
- Optimize the use of fuzzing strategies

Vulnerability by KiF
CVE-2007-4753

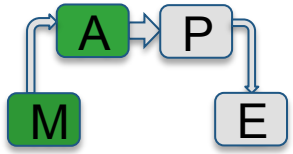
Vulnerability Discovery - Approach



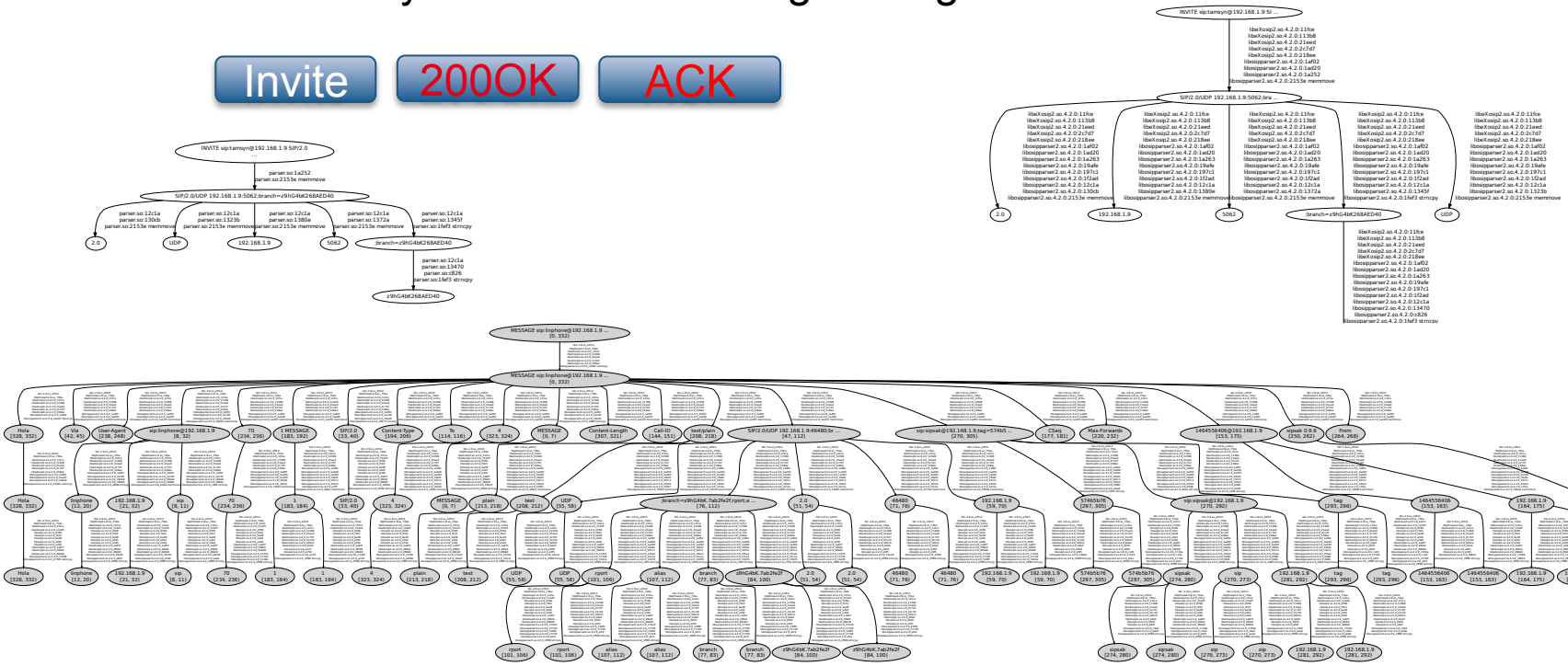
- Grey box approach
- A backtraces model for feedback collection & analysis



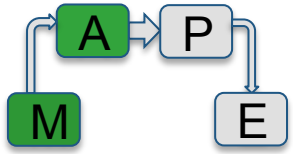
Vulnerability Discovery - Approach



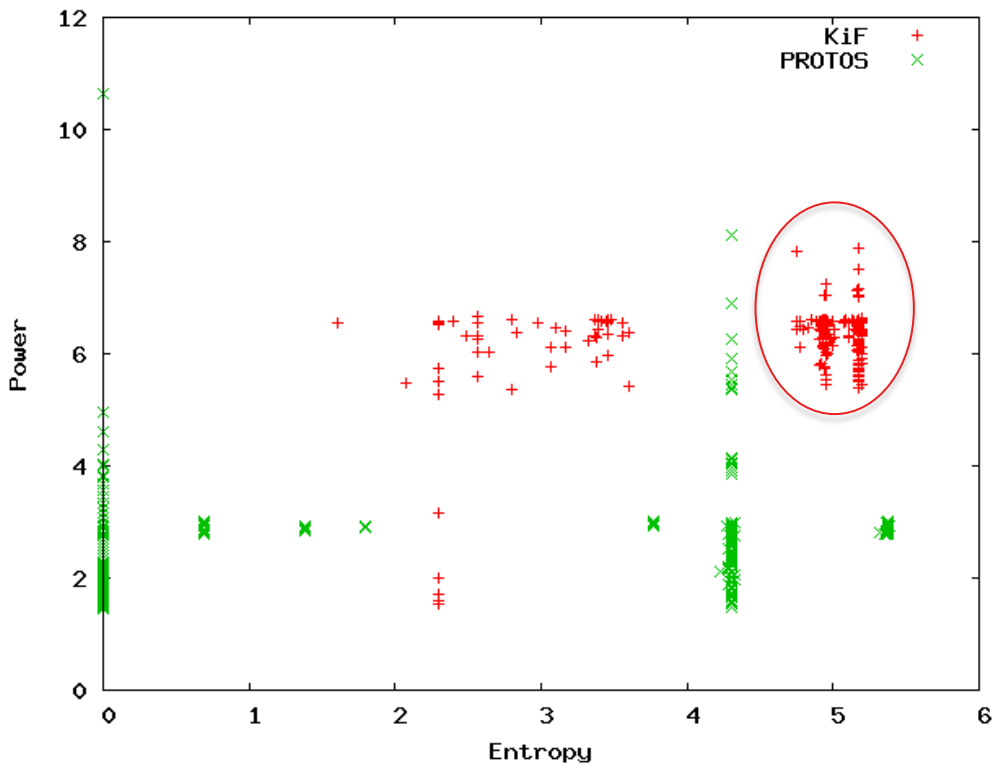
- Power & Entropy metrics to measure impact
  - Power: #values targeted by a message in one backtrace
  - Entropy: #backtraces hit bit one message
  - Link with syntax to build fuzzing strategies



Vulnerability Discovery - Impact



- A powerful model to evaluate relative impact:
  - Fuzzers
  - Fuzzing sets
  - Fuzzing Strategies
- KIF is more powerful that its competitors
  - stateful fuzzing helps
- Supported protocols
  - IPv6, PDF, DNS, DHCP, SIP, …



3

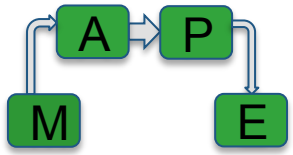
Protection against Vulnerability Exploitation

(ANR VAMPIRE, FP7 Univerself)

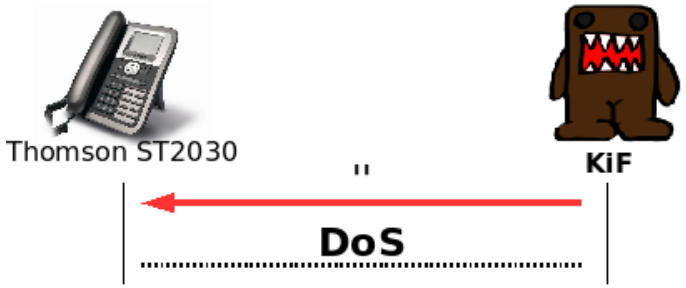
Vulnerability Exploitation Prevention - Challenge

- Context
  - Many vulnerabilities are never patched
    - No patch ever issued
    - Patch never applied in many of devices
- Challenge
  - Protect vulnerable systems
  - Automate the generation of protection policies from vulnerability descriptions
  - Design a generic prevention engine
- Achievements
  - Security automation modeling *[NOMS'12]*
  - Risk Management
    - SVM-based risk evaluation *[NassarPhD'09]*
    - Adaptive Counter-measures in SIP *[CNSM'10,11]*
      - Entreprise SIP
      - P2P SIP
      - Cloud SIP
- **Automated prevention rules generation**

Vulnerability Exploitation Prevention - Approach



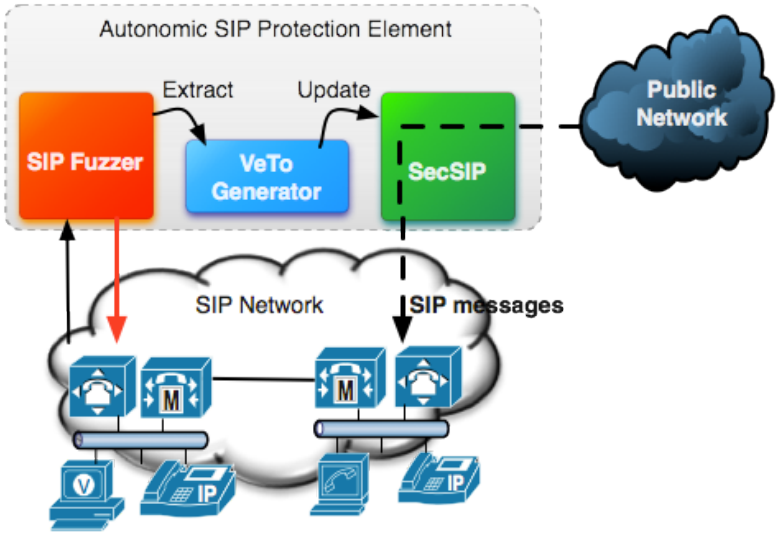
- An event-based prevention DSL *[IM'11]*
- Genetic algorithms based generation of patterns from vulnerable messages *[TNSM'12]*
- A generic prevention engine




```
veto SJPhone_Vul@SJPhone uses SJPhoneDefs begin
(ev_INVITE) -> {
            if (SIP:headers.Content_Length !@eq "SIP:body.length")
               drop; }…
```

Vulnerability Exploitation Prevention - Impact

- 0 days to protect an unpatched device
  - Through policy generation automation
- An embedded prevention engine
  - Generic
- Device specific protections activation
  - When coupled with the fingerprinting engine
  - Average 10 active rules per device
  - Rules for 16 devices



[IFIP IEEE IM'09]

Demo available during the private session !

4

Monitoring

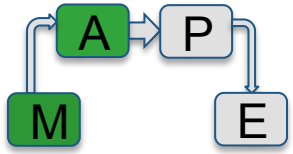
(ANR MAPE, ANR VAMPIRE, FP7 SCAMSTOP)

Network Monitoring

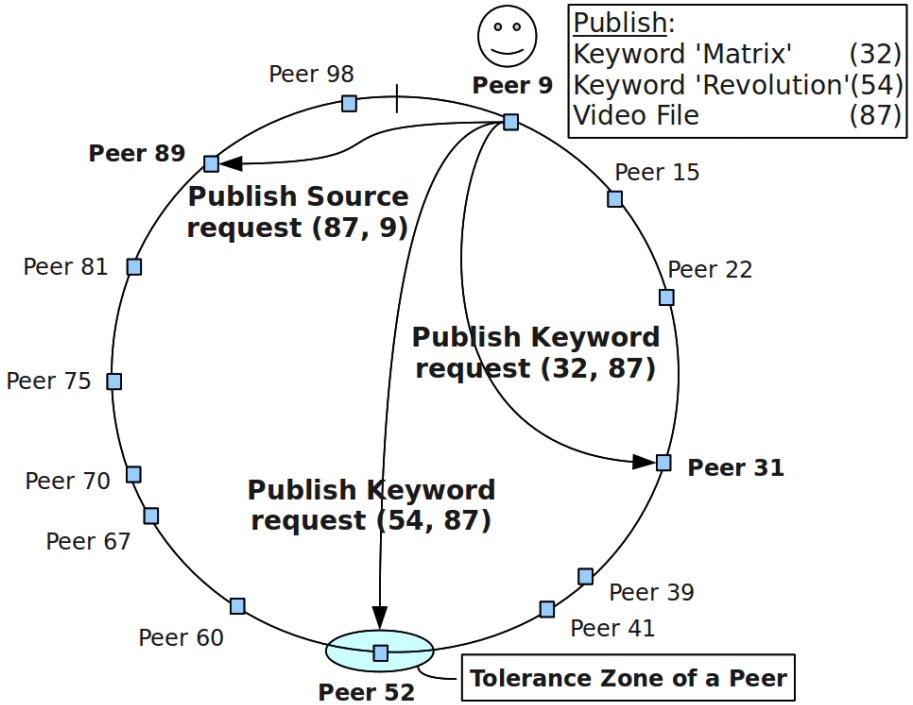
- Design probes, protocols, architecture to monitor network activities
- Detect anomalies and misuse in large scale services infrastructures
- Design efficient countermeasures

- Achievements
  - **P2P KAD Monitoring for paedophilia activity tracking** ***[P2P'11, ICC'10]***
  - VoIP signalling & Call Records based fraud detection *[RAID'08, IM'11]*
  - IPv6 automated address assignment attack protection (NDPMon) *[COMMAG'10]*

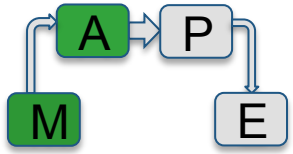
DHT-based P2P Monitoring - Challenge



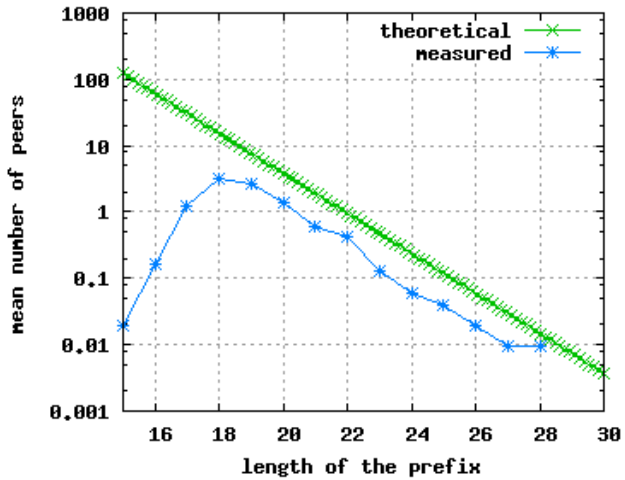
- Context
  - MAPE ANR Project : Fighting against online paedophila activity
  - Multi-network usage evaluation need
- Challenge
  - Efficient monitoring in KAD
  - Low cost monitoring prevention

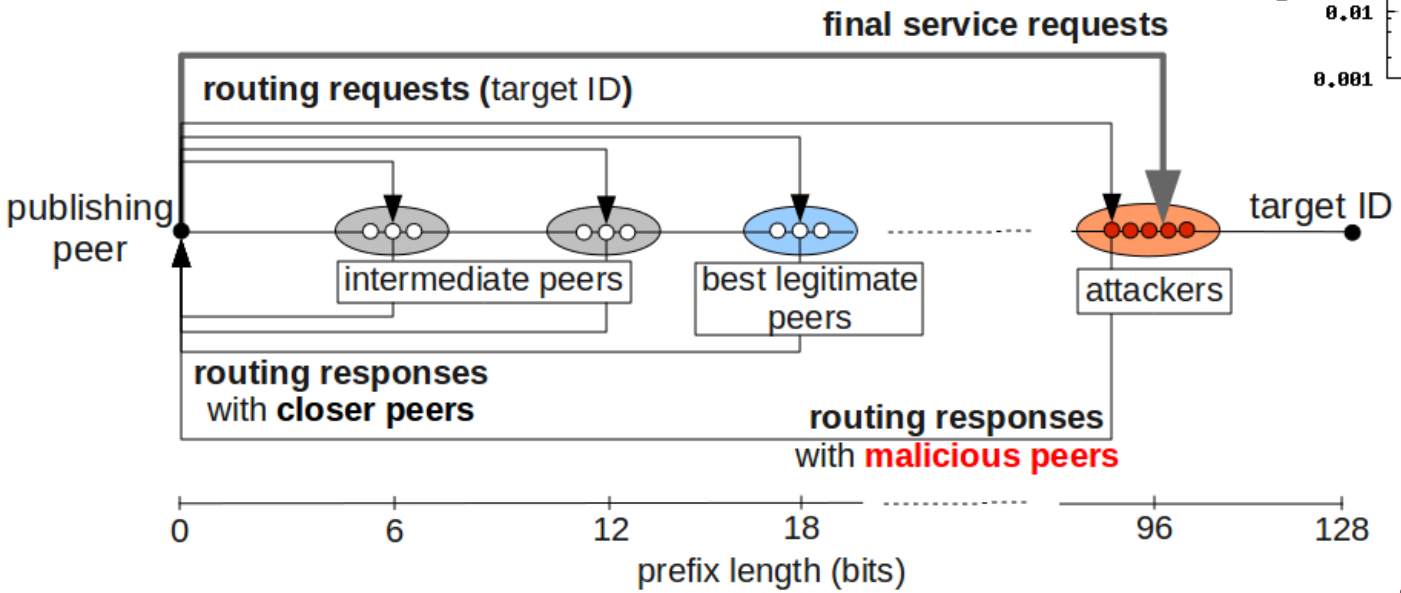


DHT-based P2P Monitoring - Approach

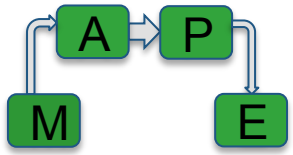


- Exploit the power of the KAD routing algorithm
- Evaluate the optimal number of probes
- Measure in the real world
- Distributed eavesdropping detection

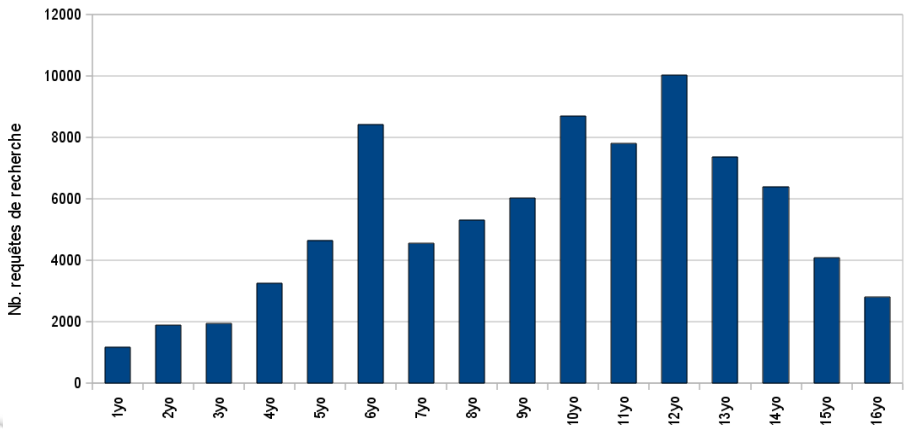




P2P KAD Monitoring: Impact



- Efficient large-scale monitoring framework for KAD
  - Validated on online child-pornography activity fighting
  - 8 campaigns of 70 keywords activity monitoring (1 week to 1 month each)
- A very powerful new protection mechanism for KAD
  - Implemented and maintained in GTK-Gnutella



5

Future Work

(2012-2015)

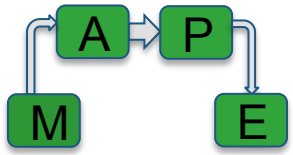
Team Evolution

Improve network management and operations in dynamic environments

- New Arrivals
  - Ye-Qiong Song
    - Mac layer design
    - Cross-layer optimizations,
    - QoS/QoA
    - Real-time networks
  - Thomas Silverston
    - Network measurment
    - IPTV
- Retirement
  - André Schaff
- External responsibilities
  - Olivier Festor, EIT ICT Labs

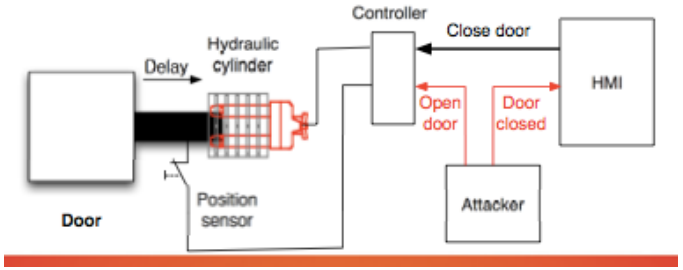
- Funding
  - 3 established funded projects until 2015
- 3 New Ph.D. Students in 2012
- The team is 8 years old

Objectives 2012-2015
Vulnerability Management

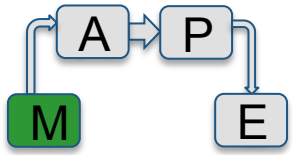


- Security automation (safe configuration)
  - Distributed vulnerability assessment
  - Cooperative vulnerability exploitation prevention

- Cyber-Physical Systems Security
  - Process-based fuzzing
  - Automated protection mechanisms generation

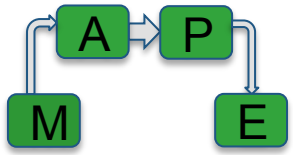


Objectives 2012-2015
Monitoring

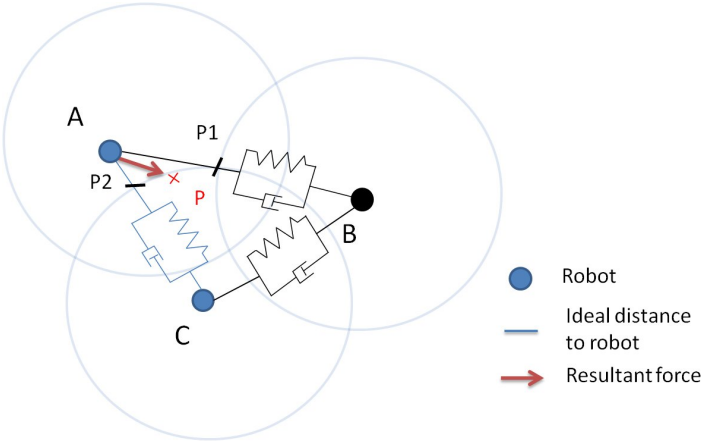


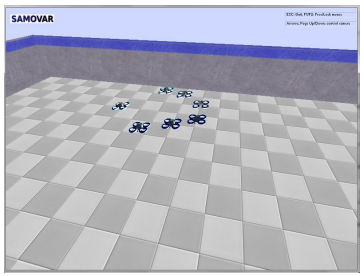
- Large scale P2P monitoring
  - Hybrid anonymous/open P2P networks monitoring
  - Impact of protection mechanisms on system performance
- Sensor networks monitoring
  - Piggy-backing protocols for management data collection
  - In-network aggregation
- Security monitoring in ICN networks
  - Design an ICN-compliant Managemement plane
  - Rethinking basic management abstractions

Objectives 2012-2015
Quality of Service & Co-Simulation



- QoS management in WSANs
  - Opportunistic & geographic routing
  - Global scheduling strategies
  - QoS-aware middleware
- Co-simulation & testbeds
  - UAVs AeTOURNOS platform





6
Summary

Summary

- MADYNES is a very active and visible team in network and service management
- Solid contributions in the reporting period
- Many more contributions to show:
  - Risk management, service discovery, co-simulation, VoIP monitoring, Security automation, …

  … will be presented & demonstrated in the private session!
- Some thematic evolutions in the future work plan
  - WSANs QoS
  - to complement existing core activities

Thank you !

NMRG
Flow Monitoring Workshop
March 31st, 2012
ICT Labs, Paris

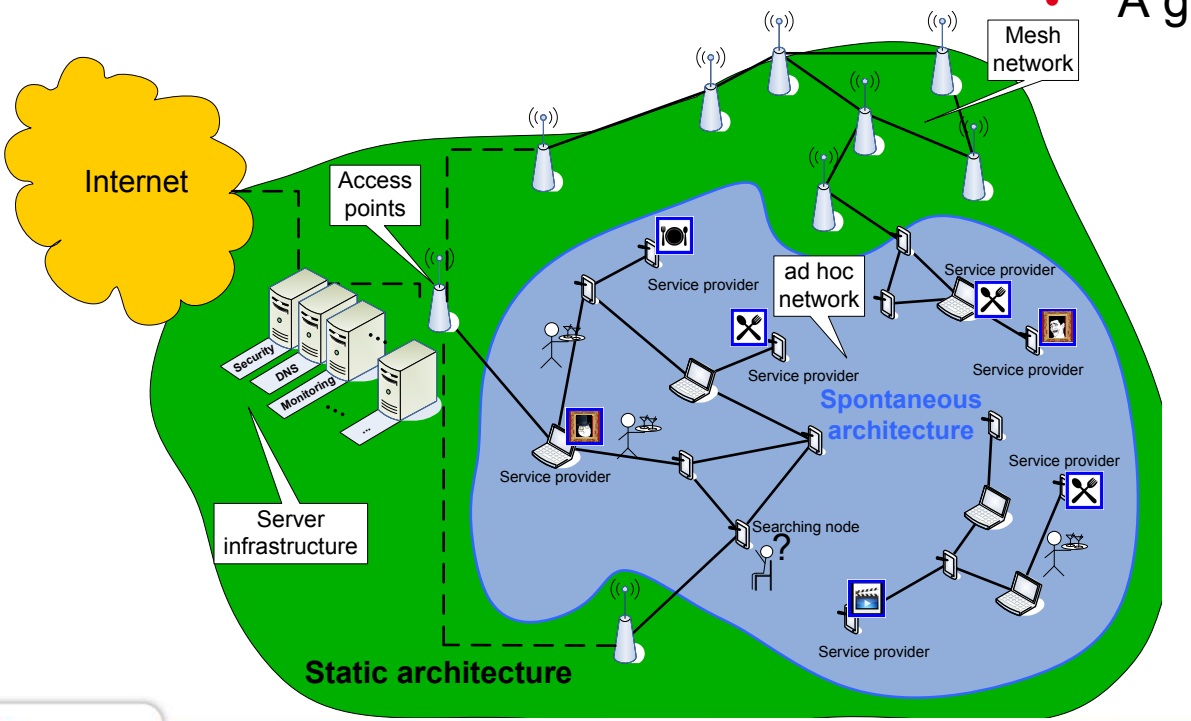
Co-Simulation and Service discovery in Smart Spaces

(ANR SARAH)

Service discovery & co-simulation in Smart Spaces : Context

Challenges

- Design and validate an efficient service discovery protocol in a Museum environment MANET

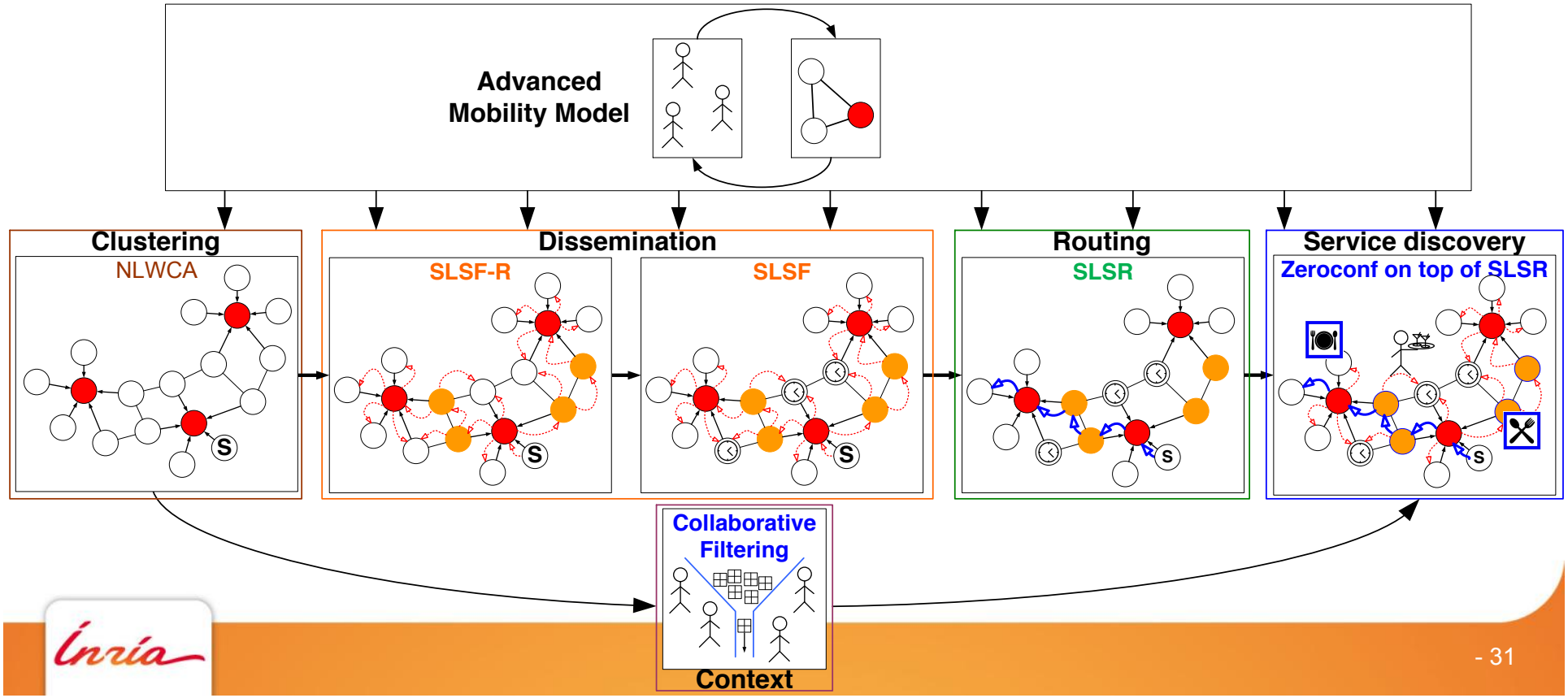


Achievements

- New cross-layer service discovery protocol for Mobile Ad hoc networks
  - SLSF + SLSR & Zeroconf
- A generic co-simulation model
  - Framework
  - Experiementation on multiple simulators coupling

Service discovery & co-simulation in Smart Spaces : Service discovery

- SLSR + SLSF
  - Protocols for routing & flooding
  - Zeroconf + collaborative filtering for service discovery



Service discovery & co-simulation in Smart Spaces : Co-simulation

- Context & behavior-aware simulation models
- Easy to integrate simulators & models