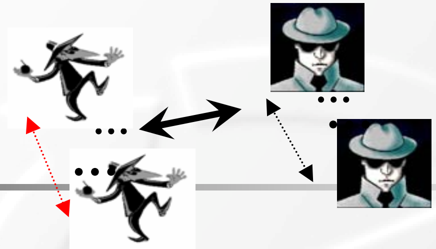


Simulation Environment for Investigation of Cooperative Distributed Attacks and Defense

Igor Kotenko, Alexander Ulanov

Computer Security Research Group,

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS)

{ivkote, ulanov}@iias.sbp.su

Goal of our Research

- The **goal of our research** is development of theoretical and practical (instrumental) basis for agent-based modeling and simulation for cyber warfare.
- The paper considers **the approach and software simulation tool** developed for comprehensive investigation of Internet DDoS attacks and defense mechanisms.
- The **simulation tool** can be characterized by three main peculiarities:
  - agent-oriented approach to simulation,
  - packet-based imitation of network security processes,
  - open library of different DDoS attacks and defense mechanisms.

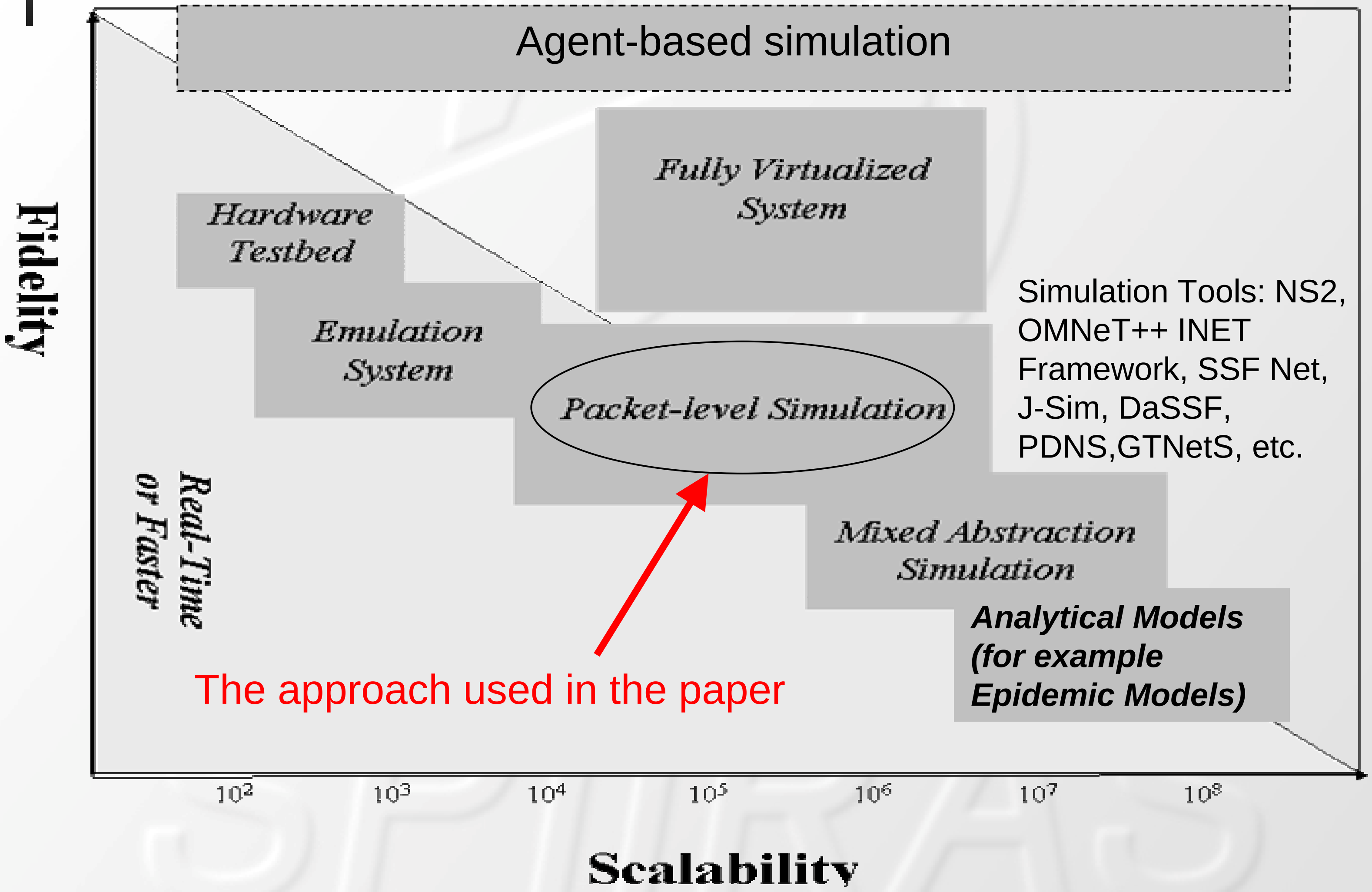
Related Works on Defense against DDoS

- The main task of defense systems against DDoS is to accurately detect these attacks and quickly respond to them [Xiang, Zhou, 04].
- It is equally important to recognize the legitimate traffic that shares the attack signature and deliver it reliably to the victim [Mirkovic, et al., 05].
- Traditional defense include detection and reaction mechanisms [Xiang, et al., 05].
- Different network characteristics are used for detection of malicious actions (for example, the source IP address [Peng , et al., 05], the traffic volume [Gil, Poletto, 03], and the packet content [Papadopoulos, 03]).
- To detect the abnormal network characteristics, many methods can be applied (for instance, statistical [Li, et al., 05], cumulative sum, pattern matching, etc).
- As a rule, the reaction mechanisms include filtering [Park, Lee, 01], congestion control [Mahajan, et al., 02] and traceback [Kuznetsov, et al., 02].

Related Works on Defense against DDoS by Cooperative Actions

- Active Security System, comprising components that actively cooperate in order to effectively react to a wide range of attacks [Canonico,et al., 01].
- COSSACK [Park, Lee, 01] forms a multicast group of defense nodes which are deployed at source and victim networks.
- Secure Overlay Services (SOS) [Keromytis, et al., 03] uses a combination of secure overlay tunneling, routing via consistent hashing, and filtering.
- A collaborative DDoS defense system proposed in [Xuan , et al., 02] consists of routers which act as gateways. They detect DDoS attacks, identify and drop attack packets.
- Distributed defense system for protecting web applications from DDoS attacks [Xiang, Zhou, 03] is deployed in both victim and attacker source end.
- DefCOM (Defensive Cooperative Overlay Mesh) [Mirkovic, et al., 05] is a peer-to-peer network of cooperative defense nodes. When an attack occurs, nodes close to the victim detect this and alert the other nodes. Core nodes and those in vicinity of attack sources suppress the attack traffic through coordinated rate limiting. Three categories of nodes : Alert generator; Rate limiter; Classifier.
- Perimeter-based defense mechanisms [Chen, Song, 05] are completely rely on the edge routers to cooperatively identify the flooding sources and establish rate-limit filters to block the attack traffic.
- …

Range of Simulation Alternatives



Source: [K.Perumalla, S.Sundaragopalan-04]

Related Works on Teamwork Approaches

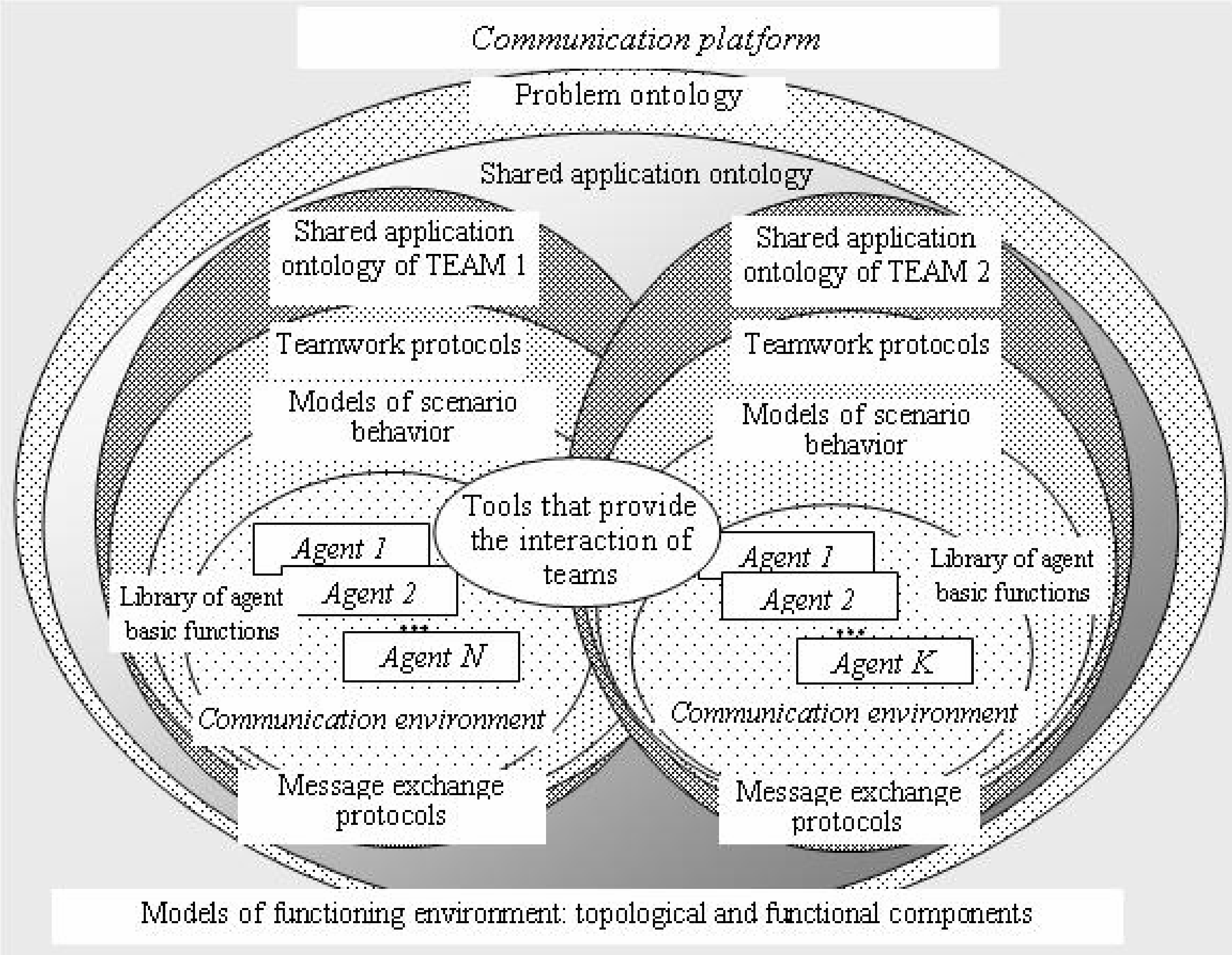
Main Agents' Teamwork Approaches:

- The **Joint intention theory** [Cohen et al., 91]
- The **Shared Plans theory** [Grosz et al., 96]
- **Combined approaches** ([Jennings,95], [Tambe,97], [Tambe et al.,01], [Paruchuri et al., 06], etc.)

Important teamwork frameworks and systems:

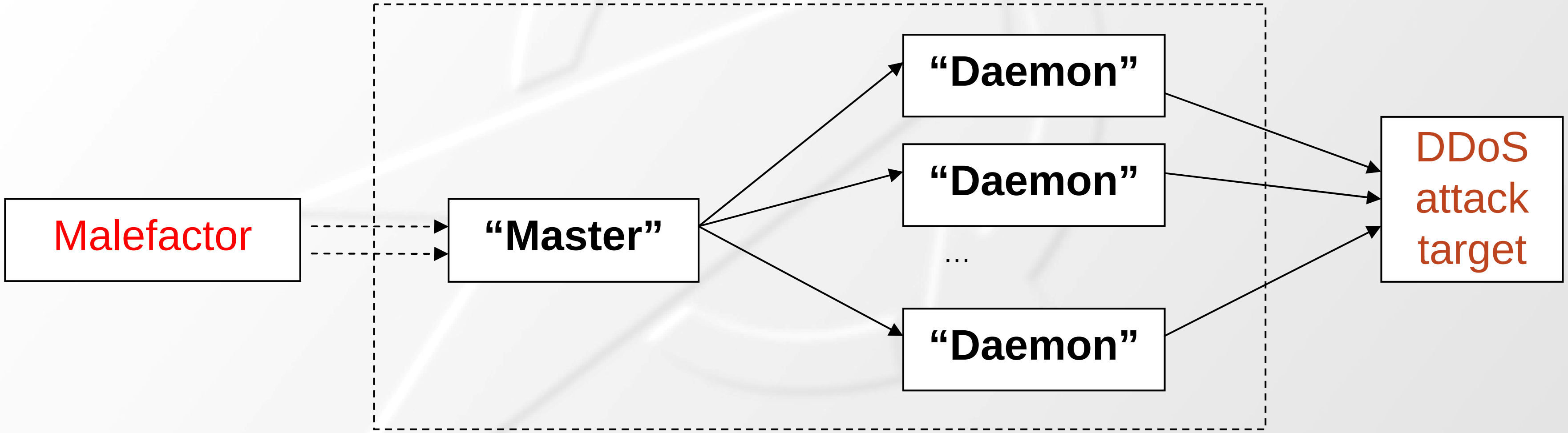
- **GRATE*** [Jennings,95]
- **OAA (Open Agent Architecture)** [Martin, et all., 99]
- **CAST (Collaborative Agents for Simulating Teamwork)** [Yen, et all., 01]
- **RETSINA-MAS** [Giampapa, Sycara, 02]
- "**Robocup Soccer**" [Stone, Veloso, 99]
- **COGNET/BATON** [Zachary, Mentec, 00]
- **Team-Soar** [Kang, 01], etc.

Abstract Model of Team Interaction

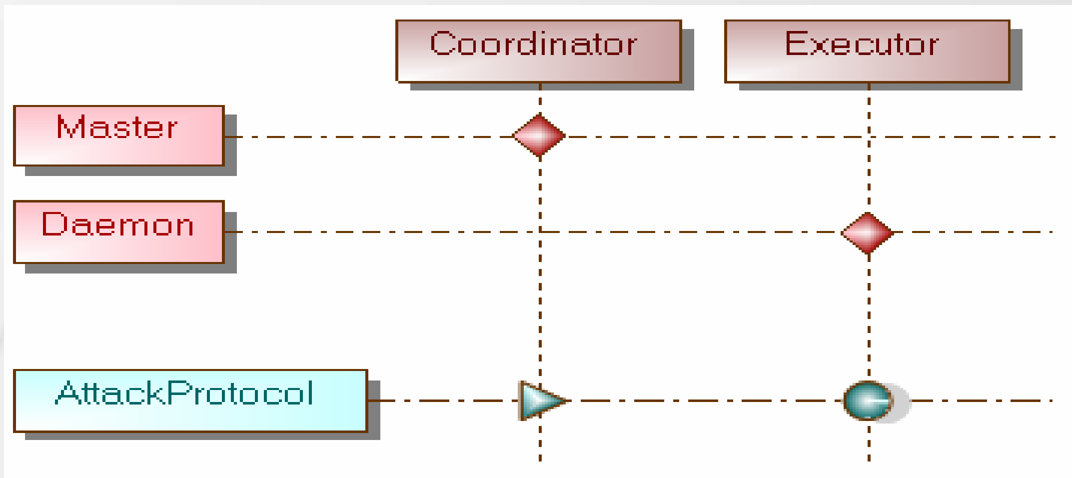


Structure and Model of Attack Team

Structure of attack team

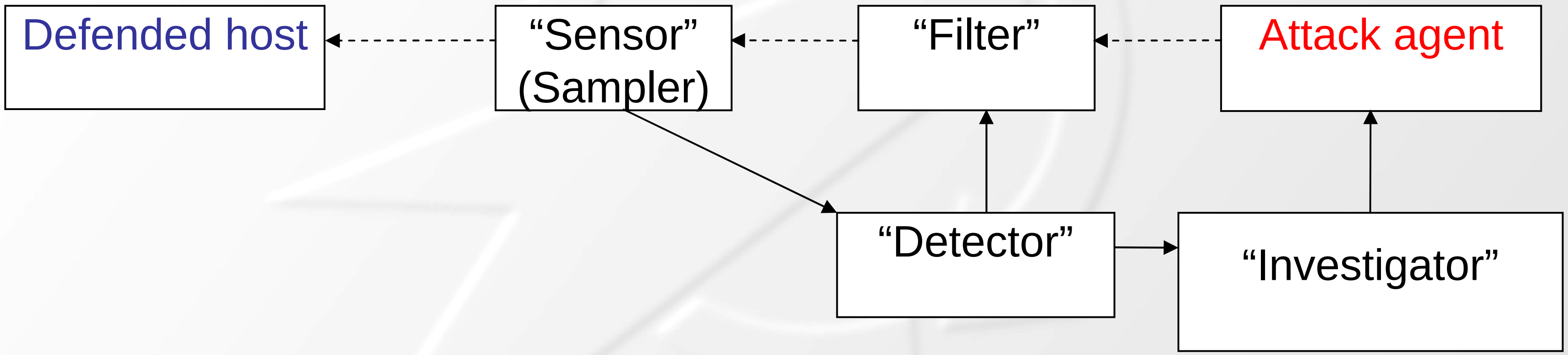


Meta-model of attack team (screenshot of meta-model editor)

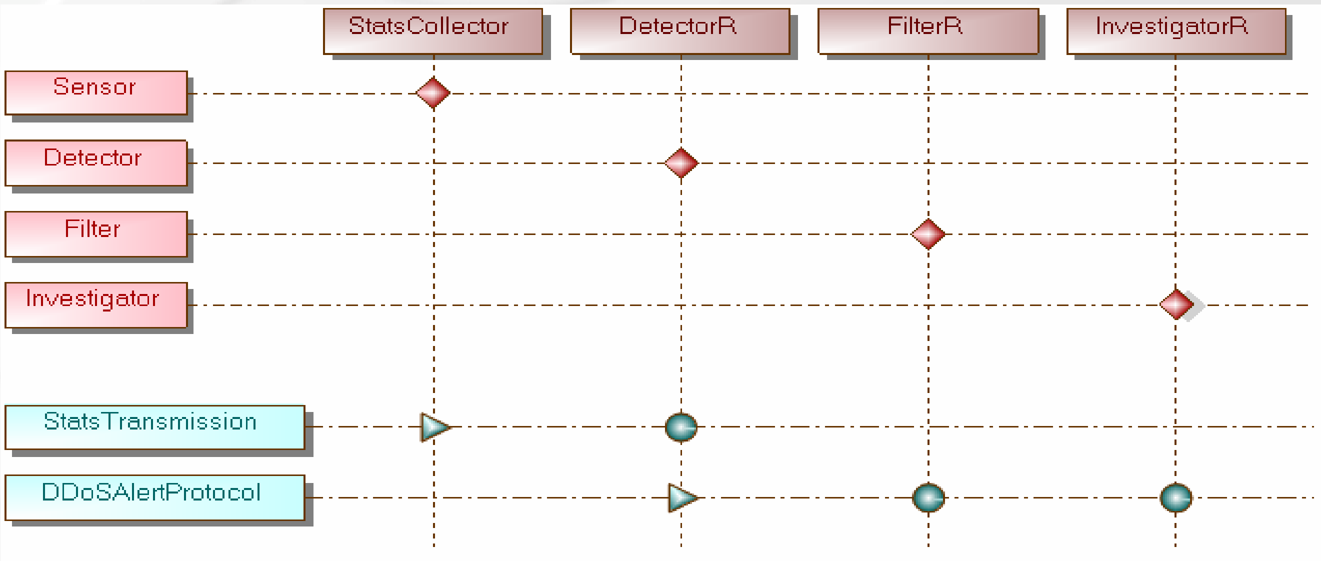


Structure and Model of Defense Team

Structure of defense team



Meta-model of defense team (screenshot of meta-model editor)



Main Classes of Attack and Defense Parameters. Parameters of Defense Efficiency

Attack module

- *Victim type*
- *Attack type*
- *Impact on the victim*
- *Attack rate dynamics*
- *Persistent of agent set*
- *Possibility of exposure*
- *Source address validity*
- *Degree of automation*

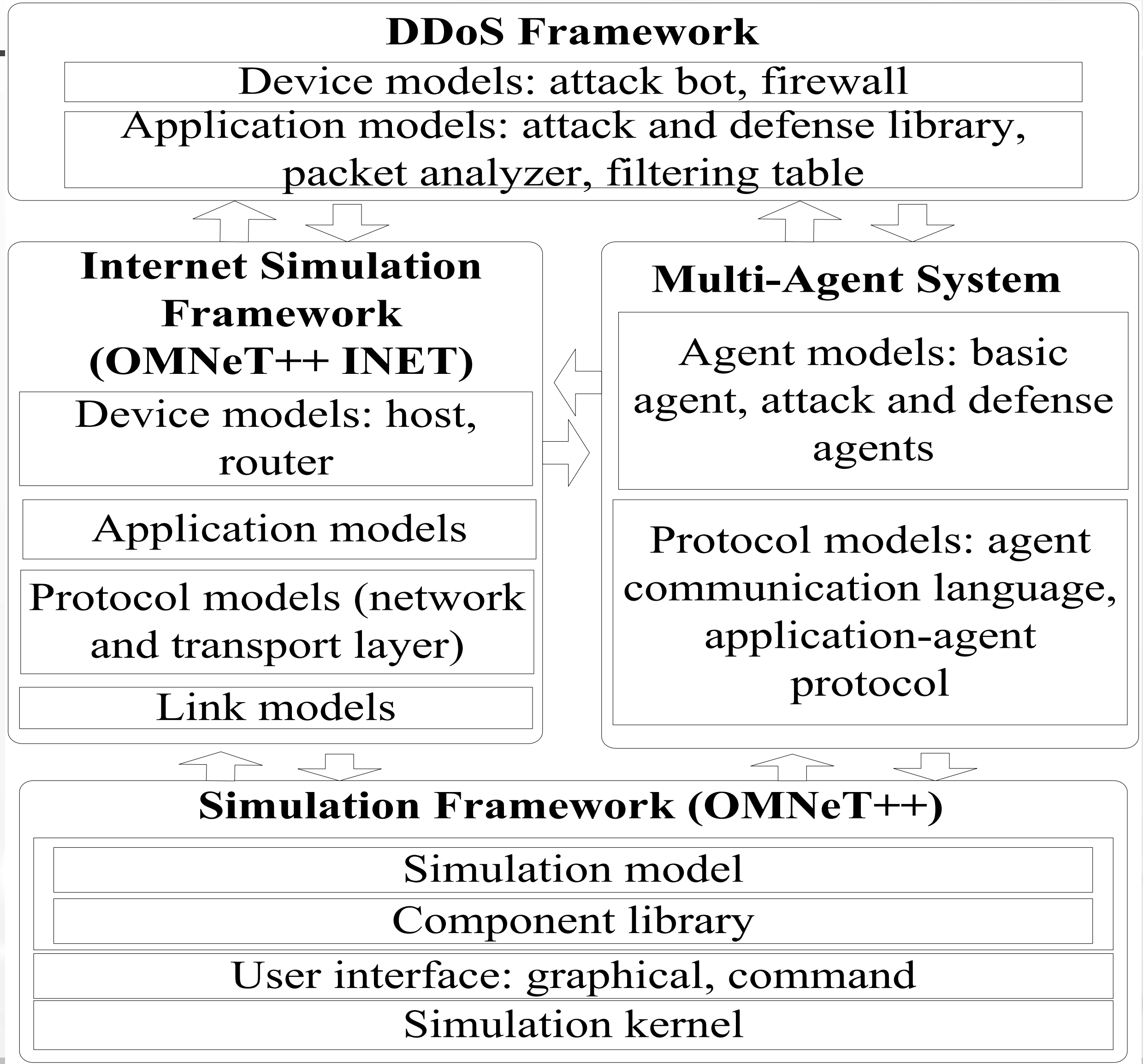
Defense module

- *Deployment location*
- *Mechanism of cooperation*
- *Covered defense stages*
- *Attack detection technique*
- *Attack source detection technique*
- *Attack prevention /counteraction technique*
- *Model data gathering technique*
- *Determination of deviation from model data*

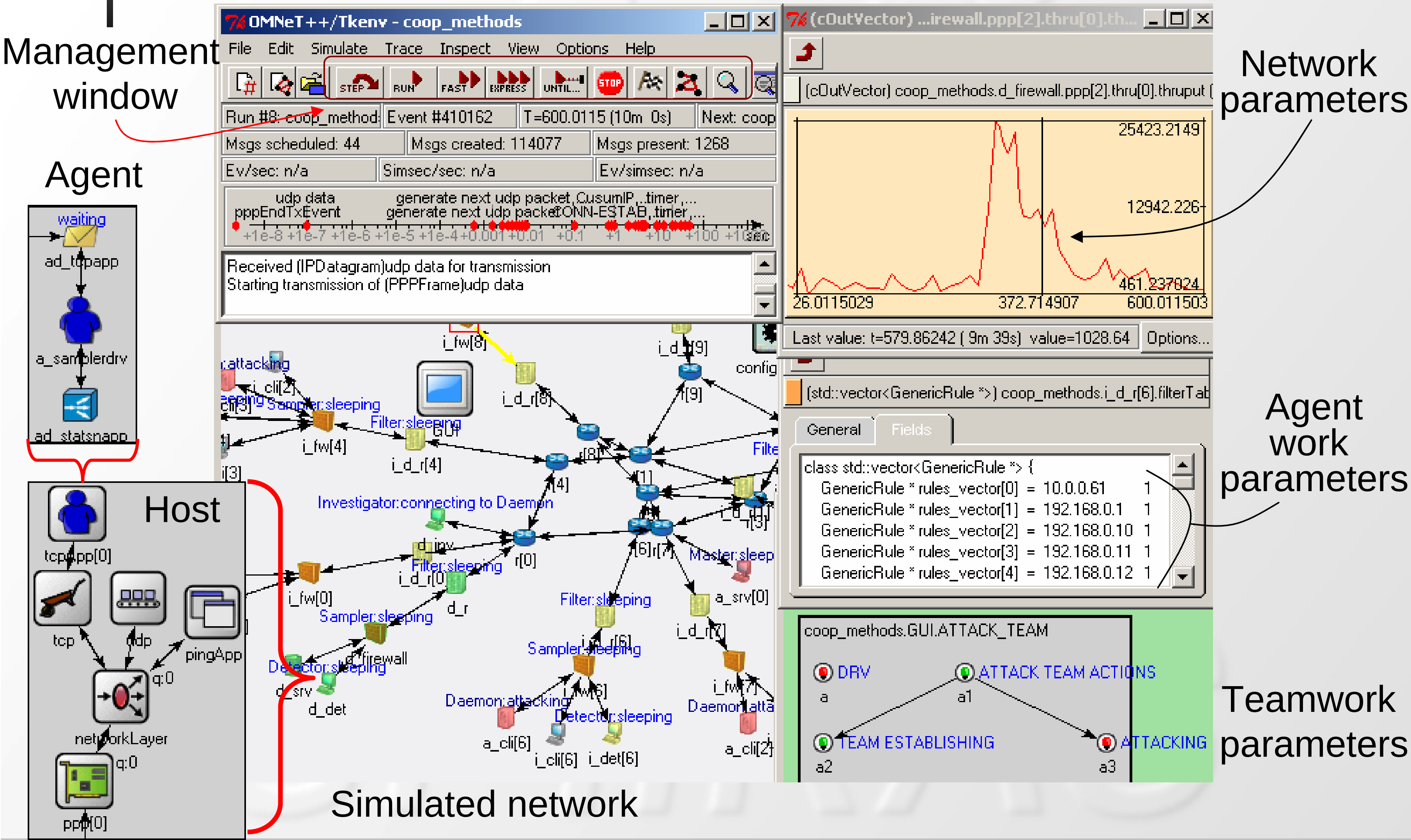
Efficiency Parameters:

- List of detectable attacks
- Volume of the input traffic before and after filters
- Percent of the normal traffic and the attack traffic on entrance to attacked network
- Rate of dropped legitimate traffic (false positive rate)
- Rate of admitted attack traffic (false positive rate)
- Attack detection and attack reaction times
- Computational complexity
- etc.

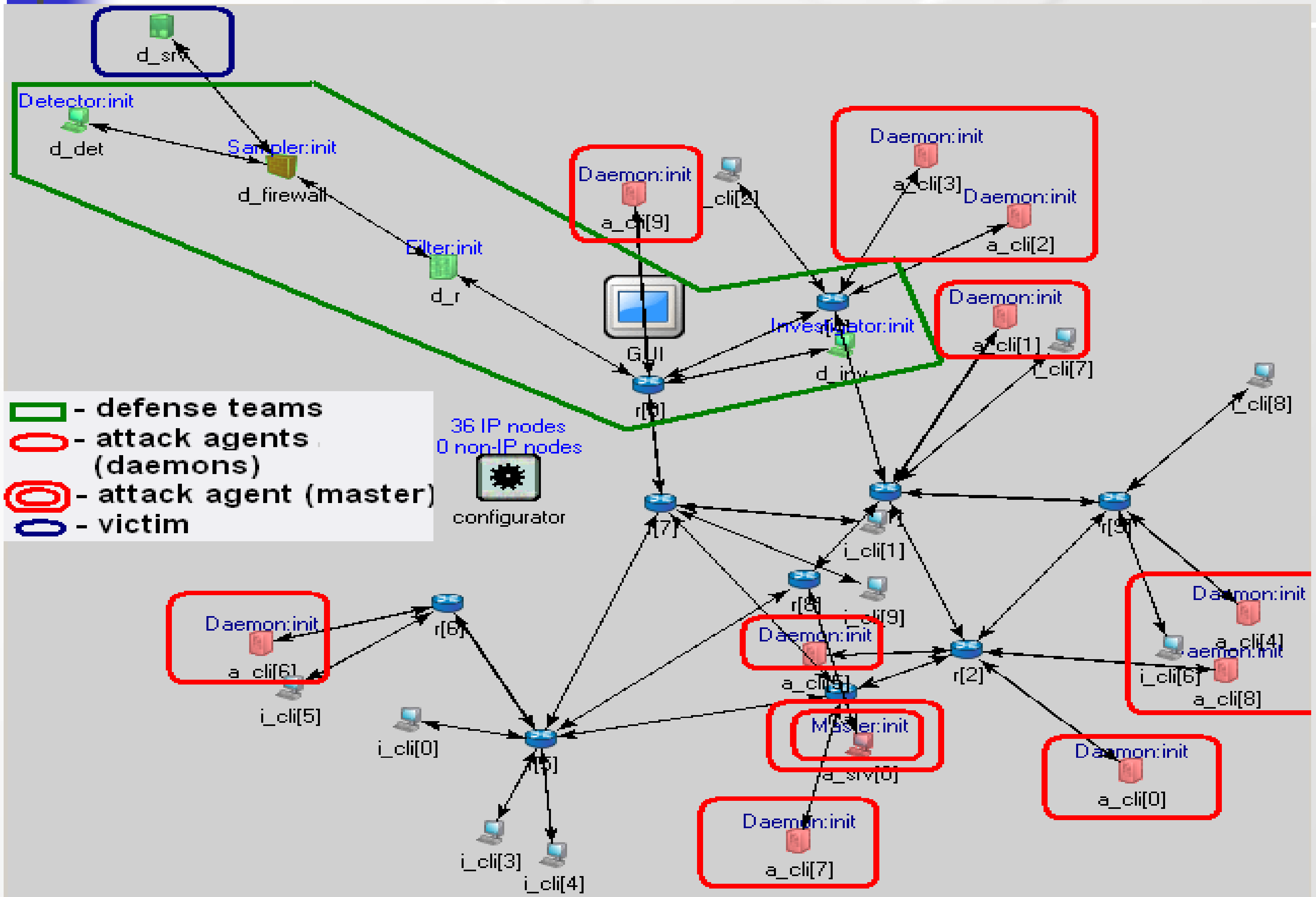
Architecture of Simulation Environment



User Interface of Simulation Environment



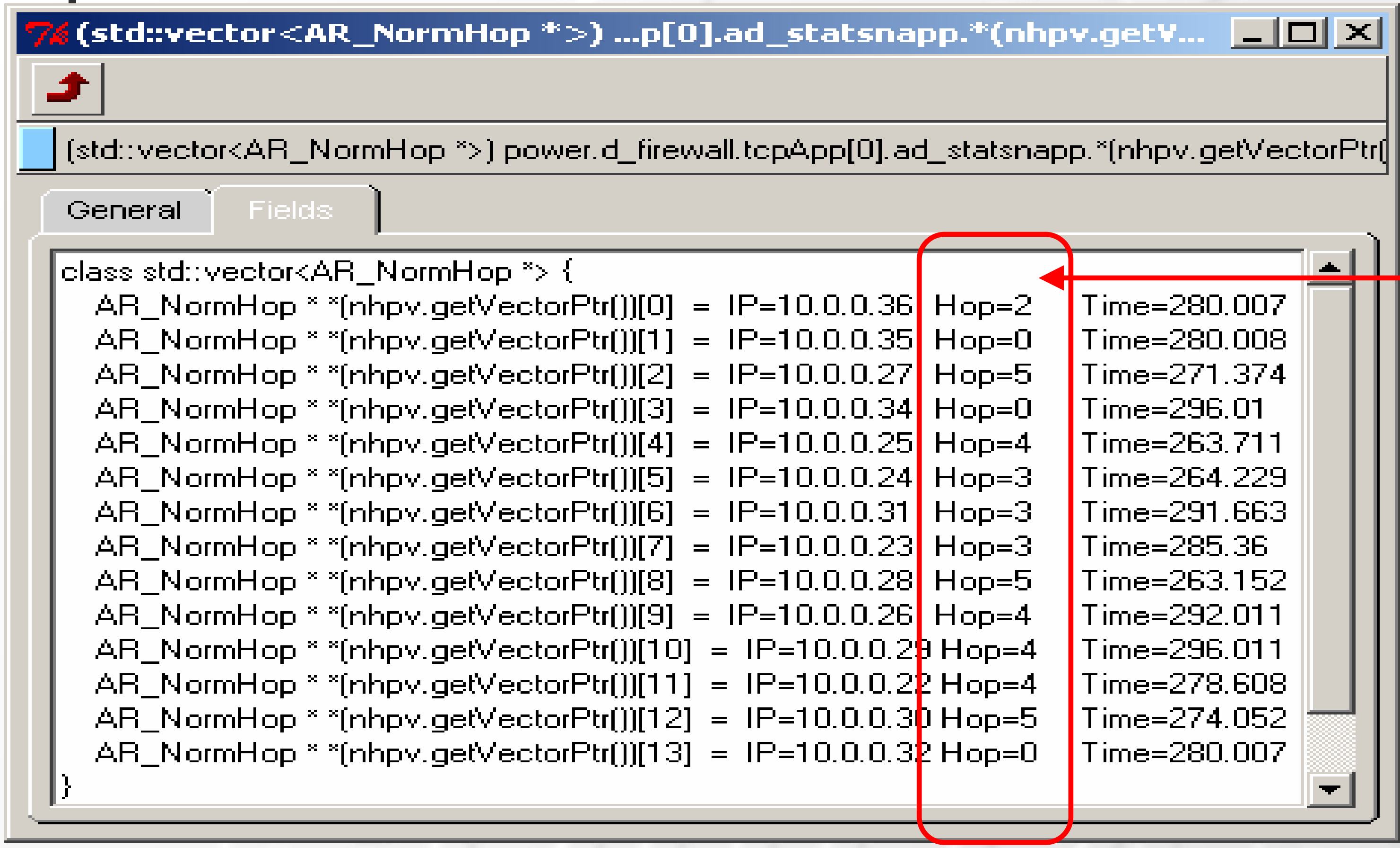
Simulation Example 1: the Internet Fragment and Agent Teams



Learning Mode (1)

- The main task of learning mode is to *create the model of generic traffic for the given network*.
- *The clients* send the requests to the server and it replies.
- At this time *sampler* analyses requests and uses them to form the models and parameters for defense different methods.
- During the learning it is possible to watch the *change of traffic models*.

Learning Mode (2)



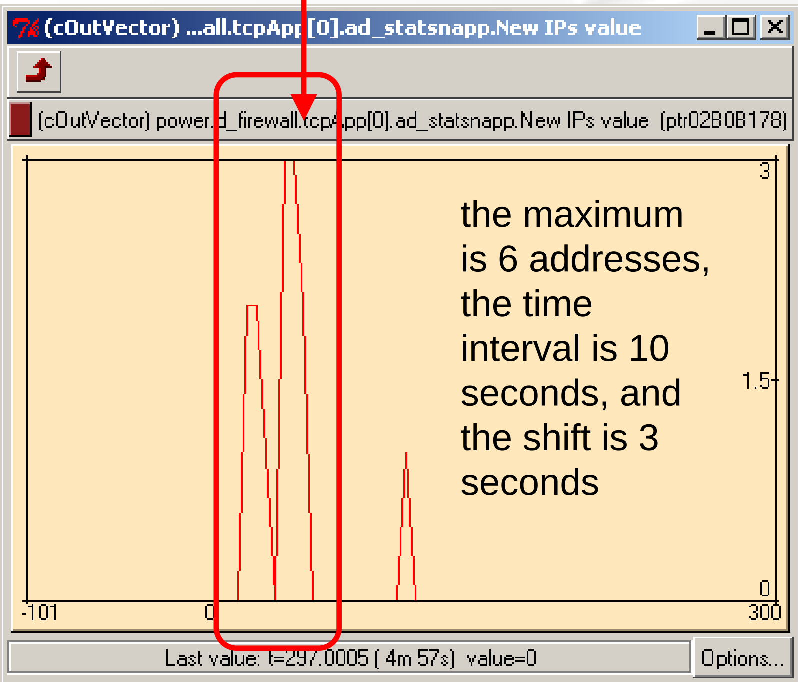
Number of hops

List of hosts that sent requests to server and <u>hops</u> to them after 300 sec of learning

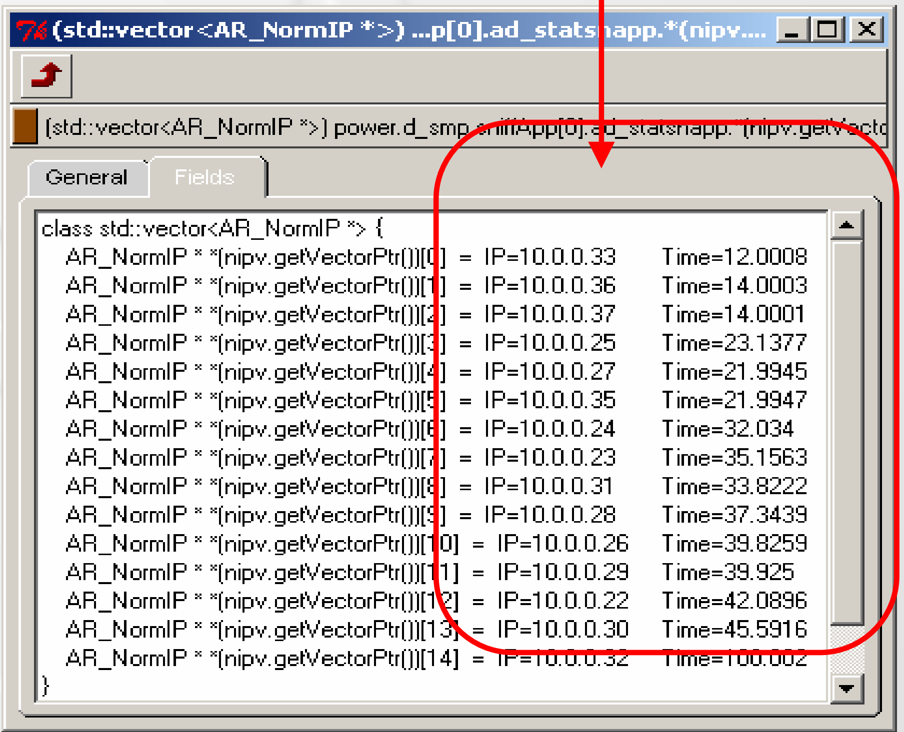
Learning Mode (3)

many new addresses in the beginning

many new addresses in the interval between 0 and 50 seconds



the maximum is 6 addresses, the time interval is 10 seconds, and the shift is 3 seconds



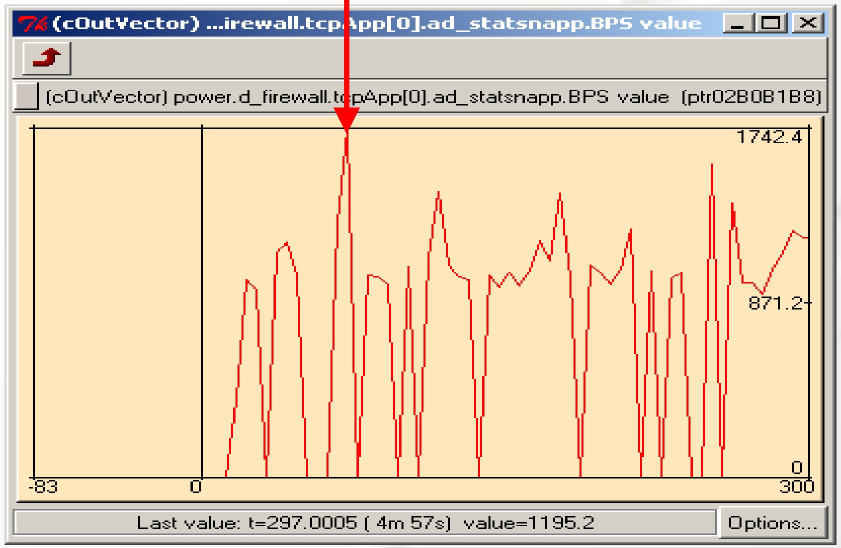
Change of new IP addresses amount

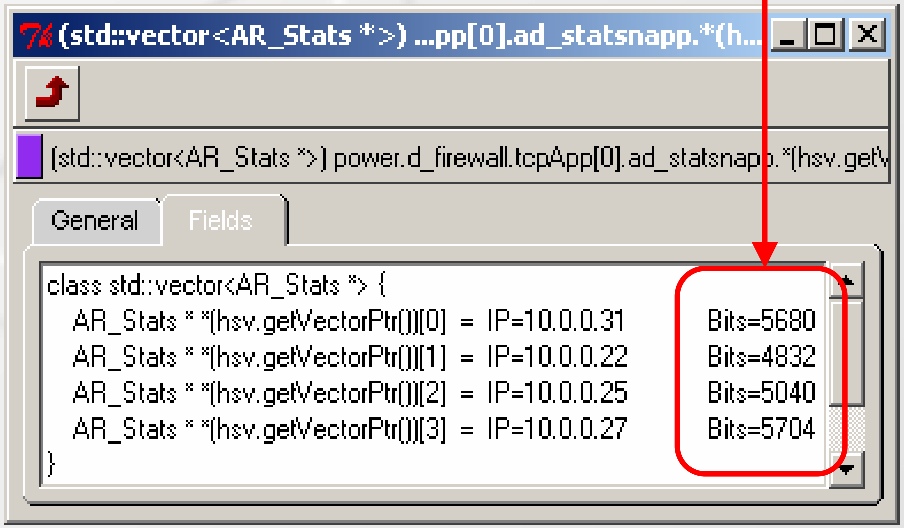
List of clients requested server and considered as legitimate after 300 sec of learning

Learning Mode (4)

The maximum value was 1742.4 bit/s

Values of bits in interval 10 seconds





Change of BPS (bit per second) parameter

Values of transmitted bits for different hosts

Decision Making and Acting

- Normal work (interval 0 – 300 seconds)

- **Defense team**: Formation, start using BPS method

- **Attack team**: Formation; After 300 seconds - begins the attack actions (intensity of attack for every daemon - 0.5, **no IP spoofing**)

- **Defense team**: Data processing, attack detecting (**using BPS**) and reacting (interval 300 – 350 seconds); Blocking the attack, destroying some attack agents (interval 300 – 600 seconds)

- **Attack team**: After 600 seconds - **automatic adaptation** (redistributing the intensity of attack (0.83), changing the method of **IP spoofing (Random)**)

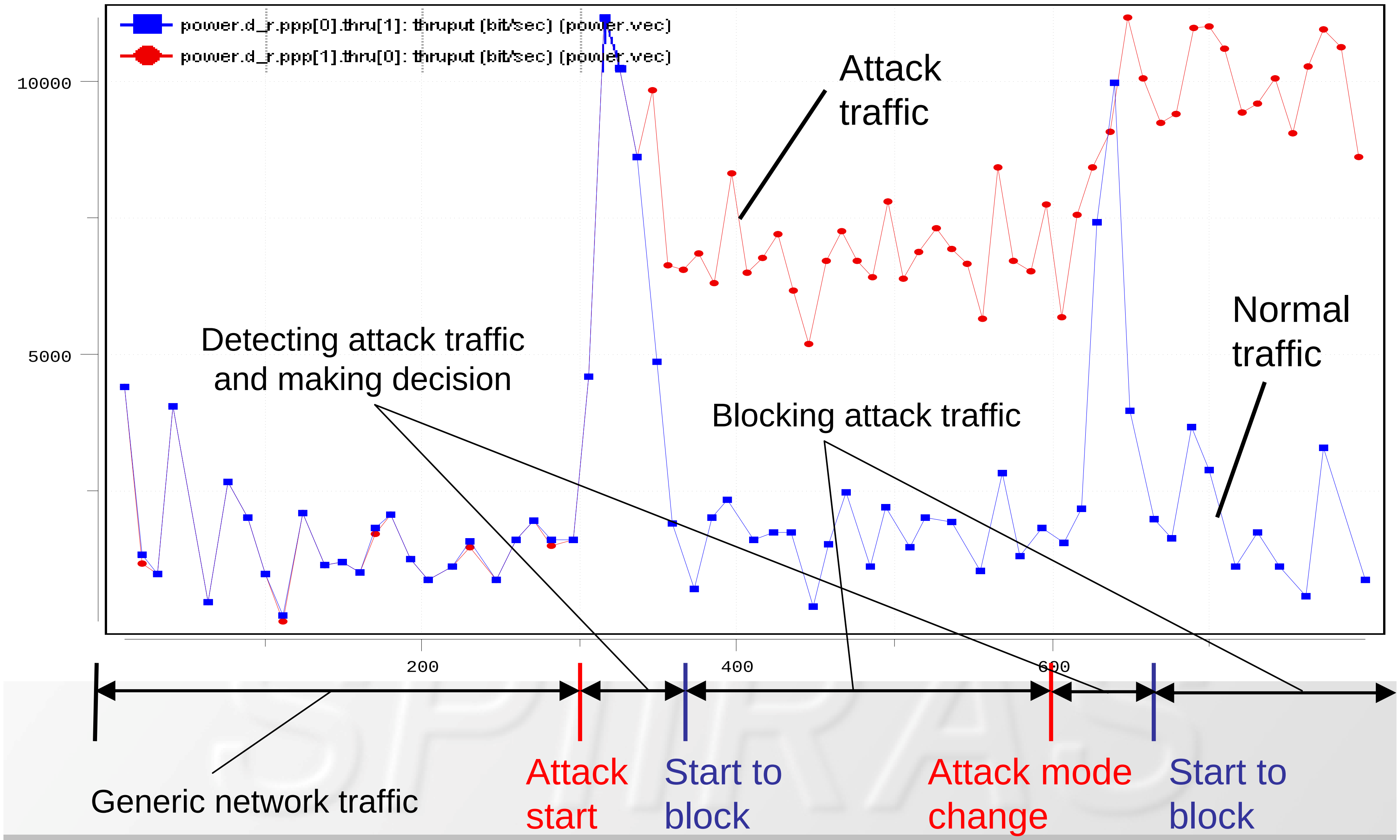
- **Defense team**: data processing, failing to detect the attack (**using BPS method**) – Detector sees that the input channel throughput has noticeably lowered, but does does not receive any anomaly report from sampler because BPS does not work.

- **Defense team**: Changing defense method on **SIPM (automatic adaptation);** Data processing, attack detecting (**using SIPM method**) and reacting – (interval 600 – 700 seconds)

…………………………..

Scheme of Acting

Graphs of channel throughput



Simulation Example 2: Cooperation between defense teams

***Models of cooperation between distributed defense teams*:**

(1) *filter-level cooperation*

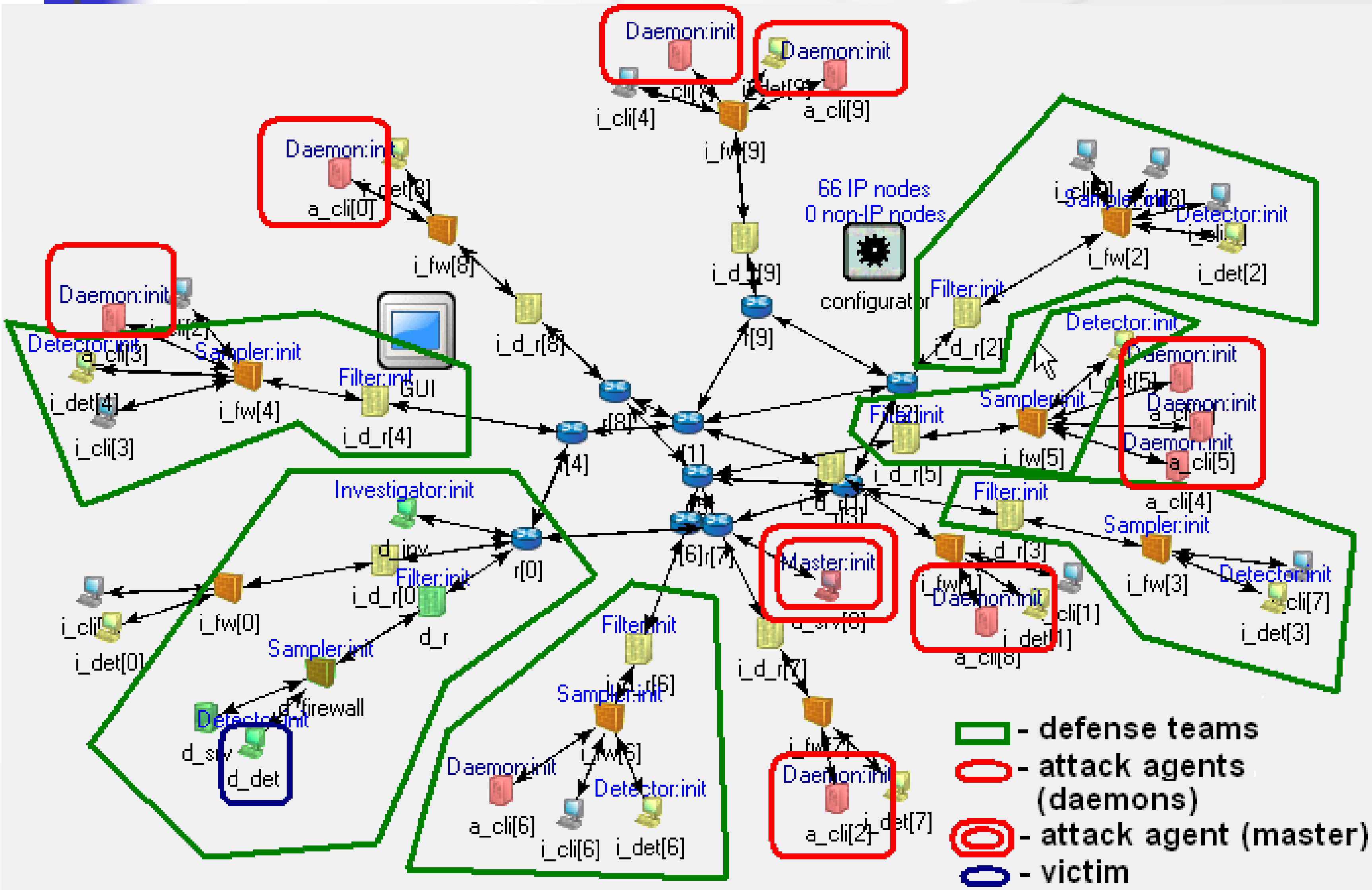
(2) *sampler-level cooperation*

(3) *"poor" cooperation*:

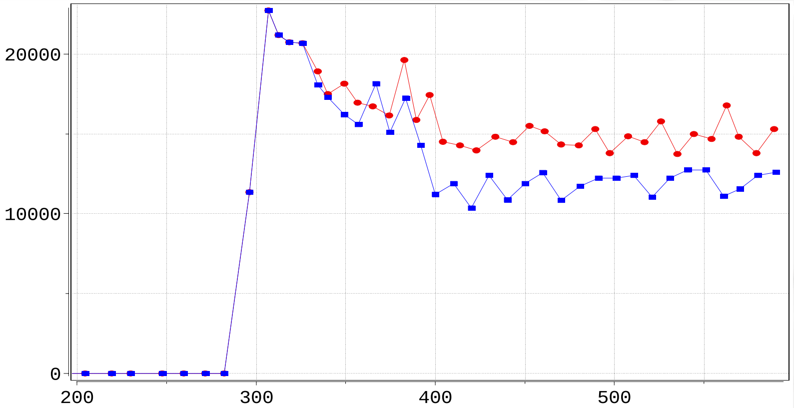
(4) *"full" cooperation*

Such cooperation schemas are used in the cooperative DDoS defense methods: COSSACK, Perimeter-based DDoS defense, DefCOM, Gateway-based, ACC pushback, MbSQD, SOS, tIP router architecture, etc.)

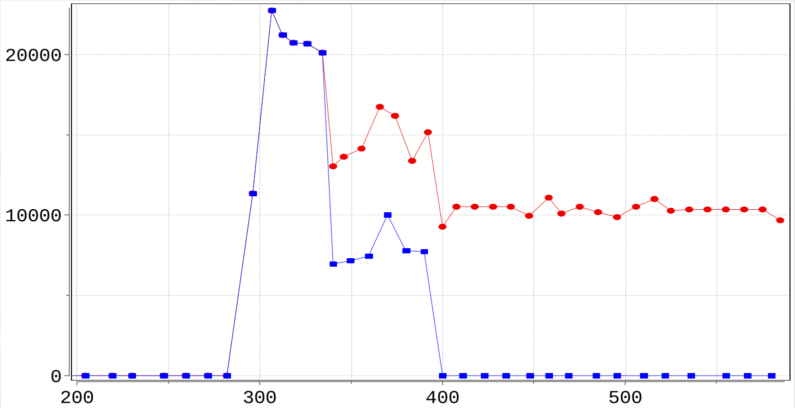
The Internet fragment and agent teams



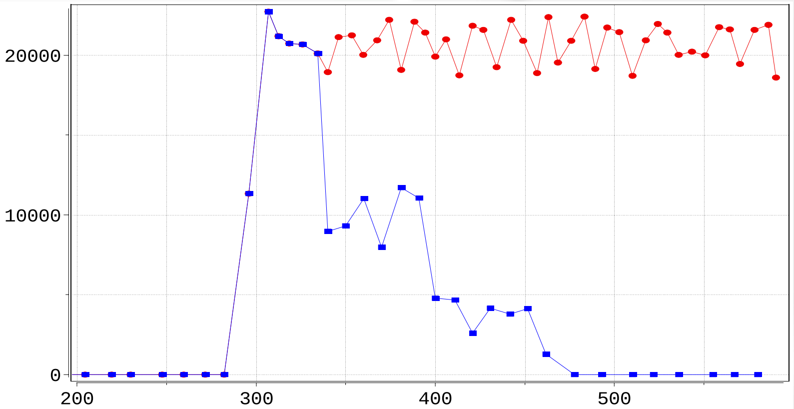
Volume of input traffic before and after the filter of the team which network is under attack (BPS)



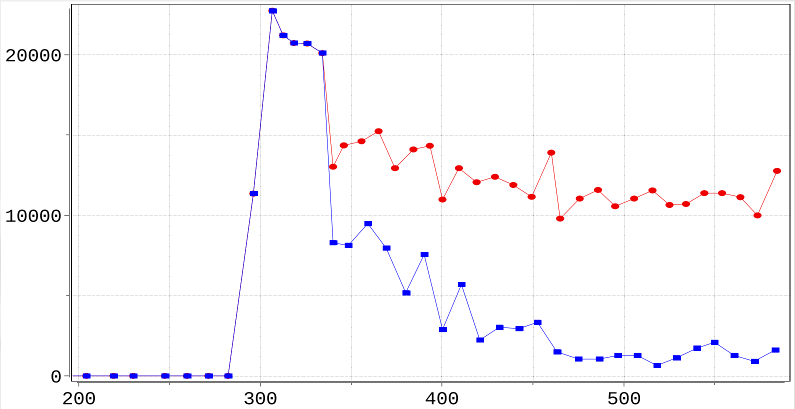
No cooperation



Filter cooperation

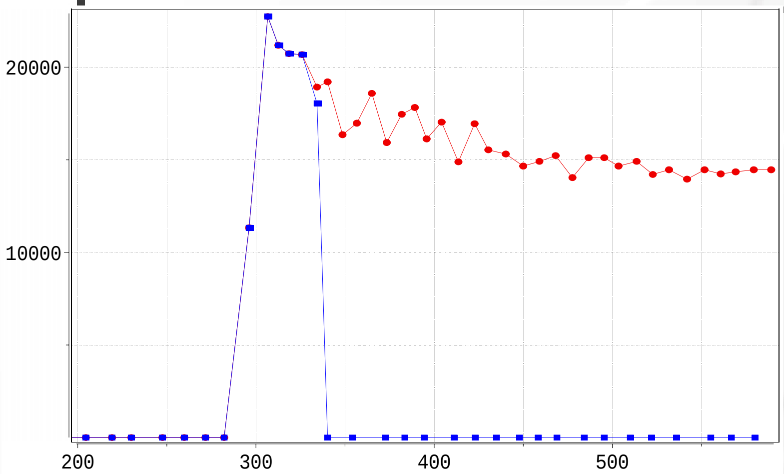


Sampler cooperation

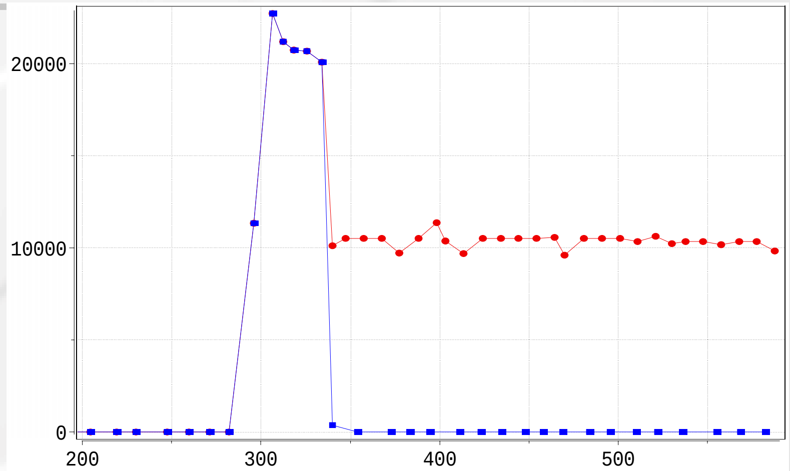


Full cooperation

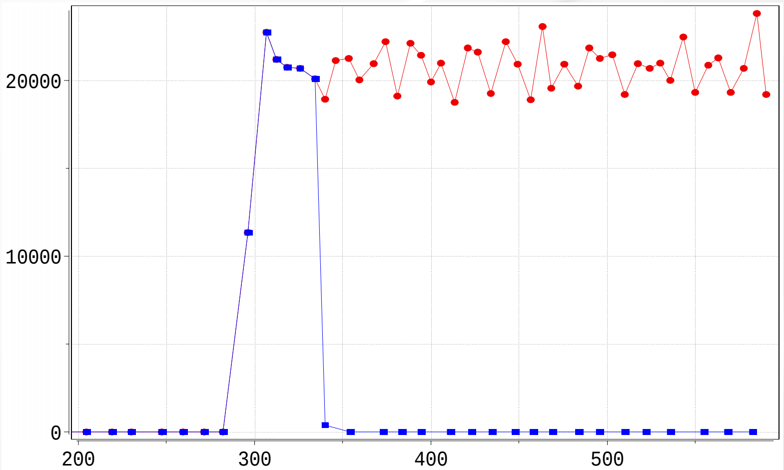
Volume of input traffic before and after the filter of the team which network is under attack (SIPM)



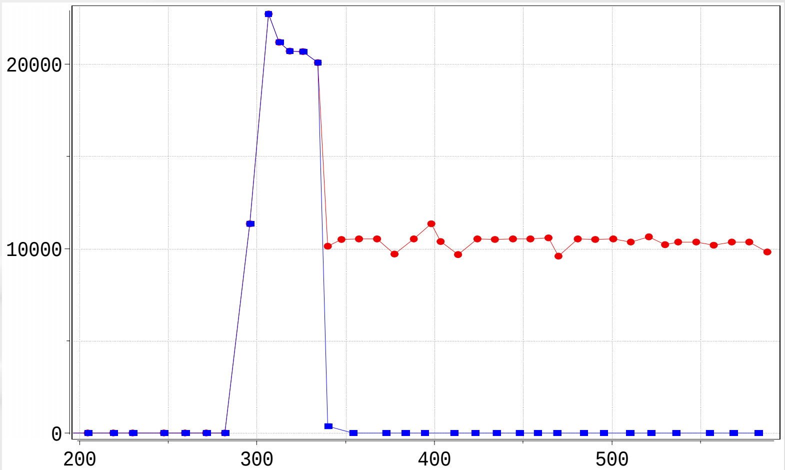
No cooperation



Filter cooperation



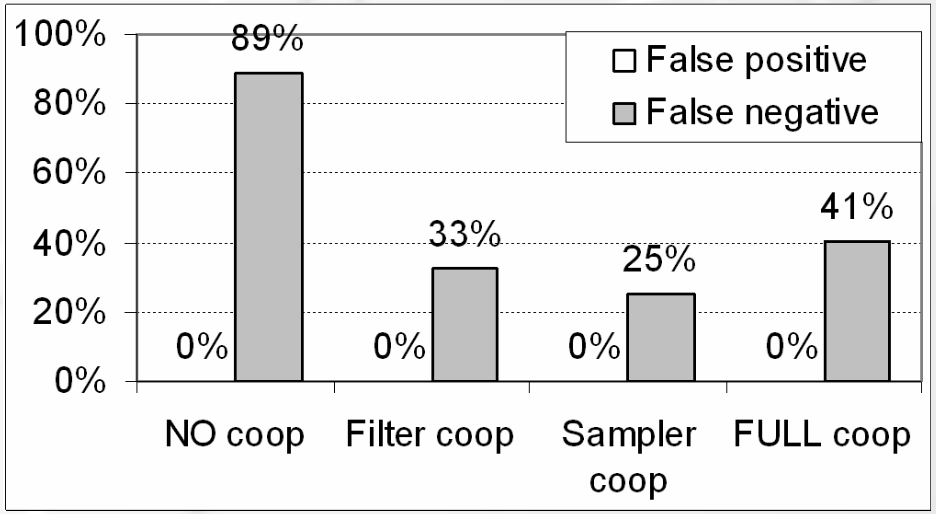
Sampler cooperation



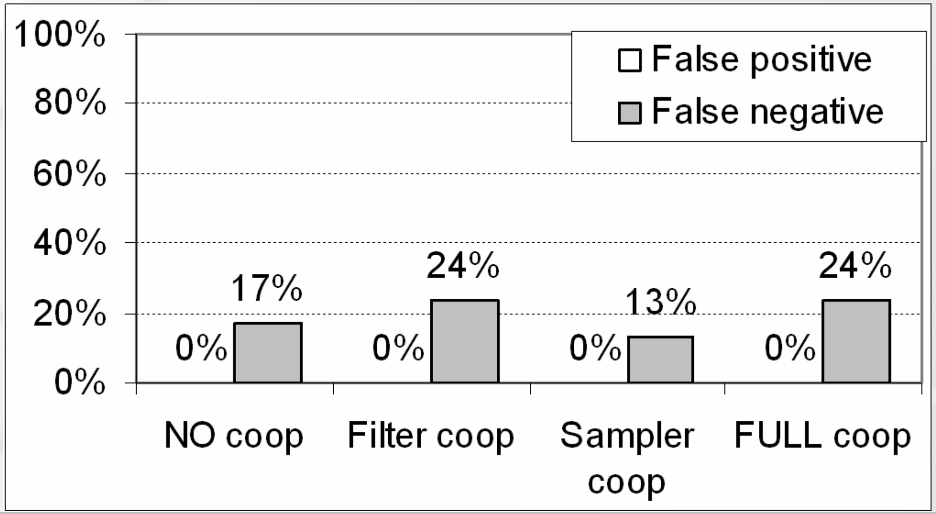
Full cooperation

False Positive and false negatives

BPS



SIPM



For more information please contact

Prof. **Igor Kotenko**

Head of Computer Security Research Group,

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS)

ivkote@iias.spb.su

http://space.iias.spb.su/ai/kotenko/

http://www.comsec.ru

Acknowledgement

This research is being supported by grant of Russian Foundation of Basic Research (№ 04-01-00167), grant of the Department for Informational Technologies and Computation Systems of the Russian Academy of Sciences (contract №3.2/03) and partly funded by the EC as part of the POSITIF project (contract IST-2002-002314).