Lack of Security Violates Quality of Service

Erol Gelenbe

Fellow of the National Academy of Technologies of France (FNATF)
Foreign Fellow of the Belgian, Hungarian and Polish Science Academies

Professor in the Dennis Gabor Chair, EEE Dept., **Imperial College London**
Professor, Institute of Theoretical and Applied Informatics, Polish Academy of Sciences
e.gelenbe@imperial.ac.uk

Imperial College London

GENERAL CONSIDERATIONS

- **CyberAttacks target Societal Infrastructures, e.g. Health, Transport, Energy, Finance, Education, Manufacturing, Supply Chains, Cities, Safety, Politics, Comfort**
- **The Internet was Designed as a Research Project by PhD Students**
- **The Origin of Traffic Cannot be Easily Identified and Traced**
- **Security and Provenance were not Part of the Initial Design**
- **Could the System be Re-Designed or Substantially Modified?**
- **Who would pay for that? Is there a Role for the EU?**

GENERAL CONSIDERATIONS

- **CyberAttacks target Societal Infrastructures, e.g. Health, Transport, Energy, Finance, Education, Manufacturing, Supply Chains, Cities, Safety, Politics, Comfort**
- **CyberDefense is About Defense & Attack Operations in CyberSpace**
- **CyberAttacks are Here to Stay for a While**
- **Everyone is Training More Human Defenders and Attackers (i.e. CyberSecurity Experts)**
- **By understanding Cyber Defense we better Understand CyberAttacks**
- **Without International Agreements and Regulations, Policing is Difficult**
- **The Internet of Things can (will?) make things much Worse …**

- **GENERAL CONSIDERATIONS**

- **CyberAttacks are primarily Conveyed by Mobile Networks, Internet, WiFi…**
- **In the First Instance they Target Networks, Servers, the Cloud**
- **Detection Schemes should monitor “traffic” continuously to respond to developing attacks with high accuracy and limited False Alarms**
- **CyberDefense must evaluate overall infrastructure resilience and adaptability in the presence of dynamically varying service requests (sometimes confused as attacks) and CyberAttacks**
- **We need to design, evaluate and make sure that we have Comprehensive Response Schemes**
- **Systems should be Resilient to CyberAttacks and False Alarms**

The Current Way Forward

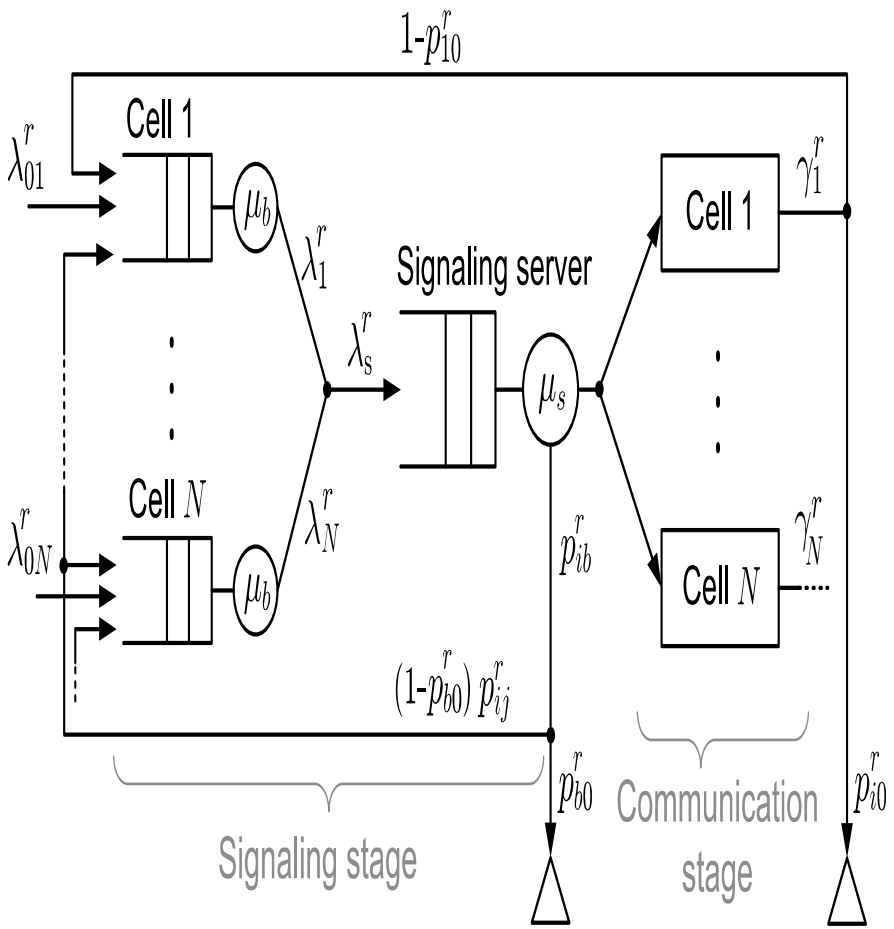
A) Detection of Attacks

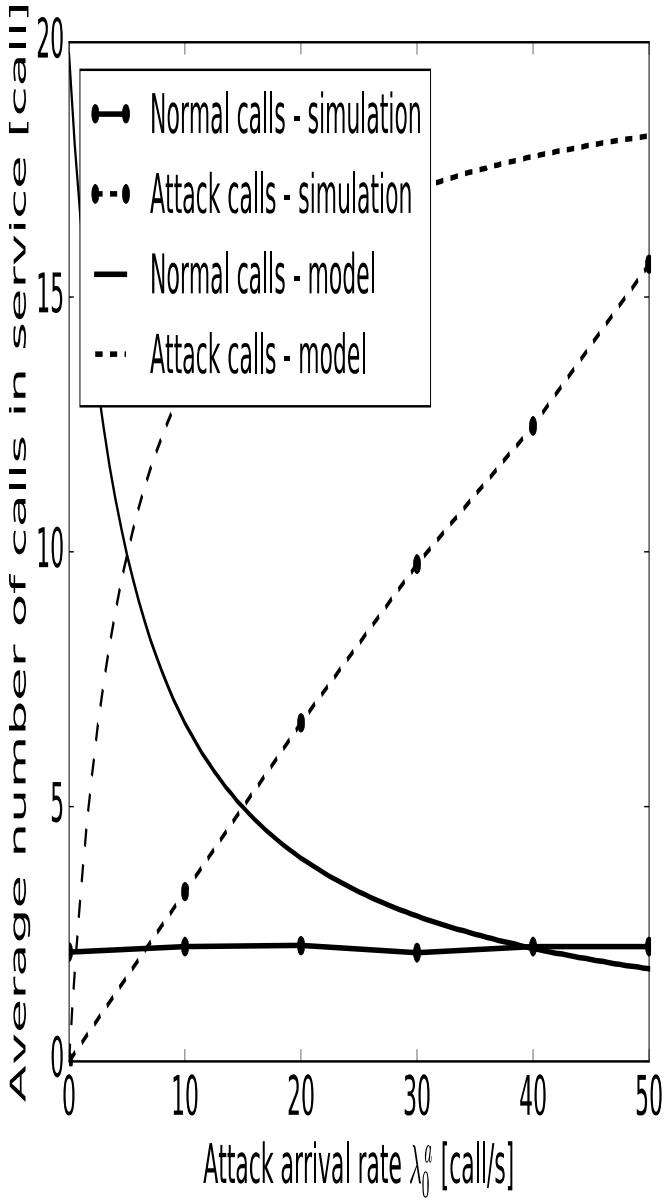
- **Detection Mechanisms**, based on monitoring traffic parameters (instantaneous and statistical) in real-time, evaluating likelihood ratios related to normal and attack traffic and decision making by the use of RNNs or other ML
- Combining detection schemes with response mechanisms for **integrated defence architectures**
- **Dynamic defence distribution scheme** which pre-assigns a role to specific nodes to re-route traffic and rate-limit or drop attack packets

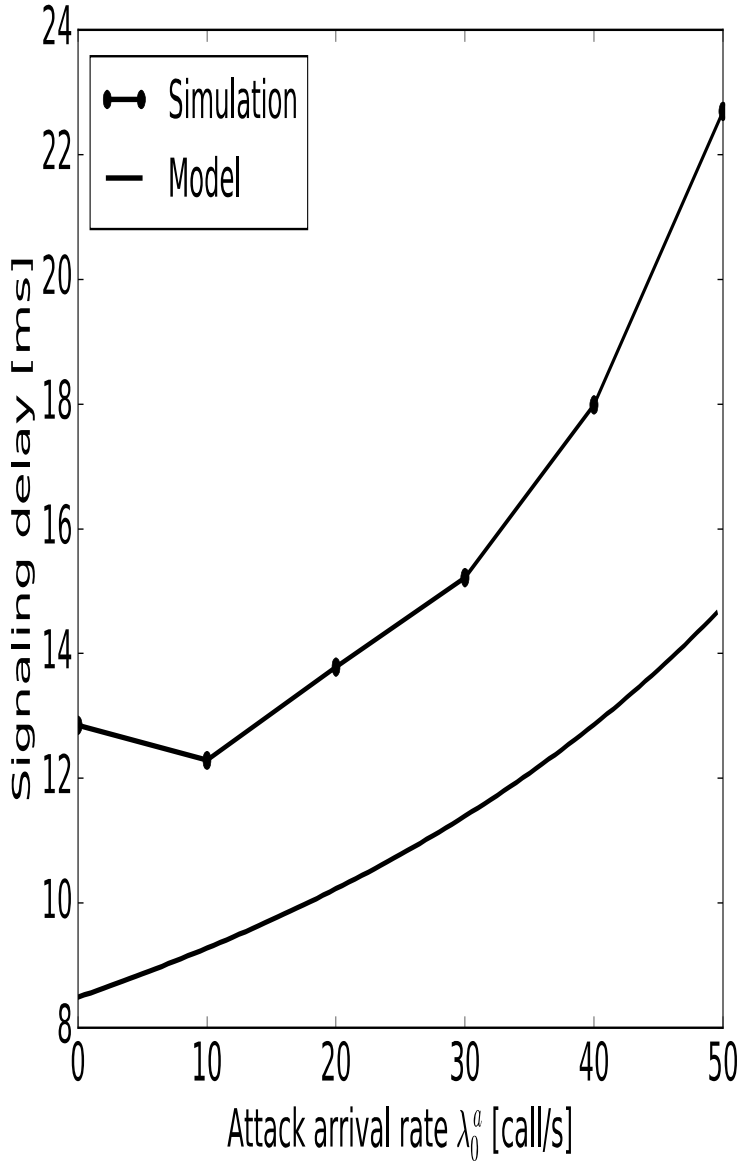
B) Stable Networks with Attacks

- Develop modelling/simulation environments for **network systems subject to attacks and catastrophic or intermittent failures**
- Mitigate **failure spreads** based rapid patching, and massive packet drops to avoid the spread of attacks
- **Response mechanisms** using autonomic network algorithms for stable network behaviour in the presence of attacks, in order to mitigate the effects of the attacks and false alarms

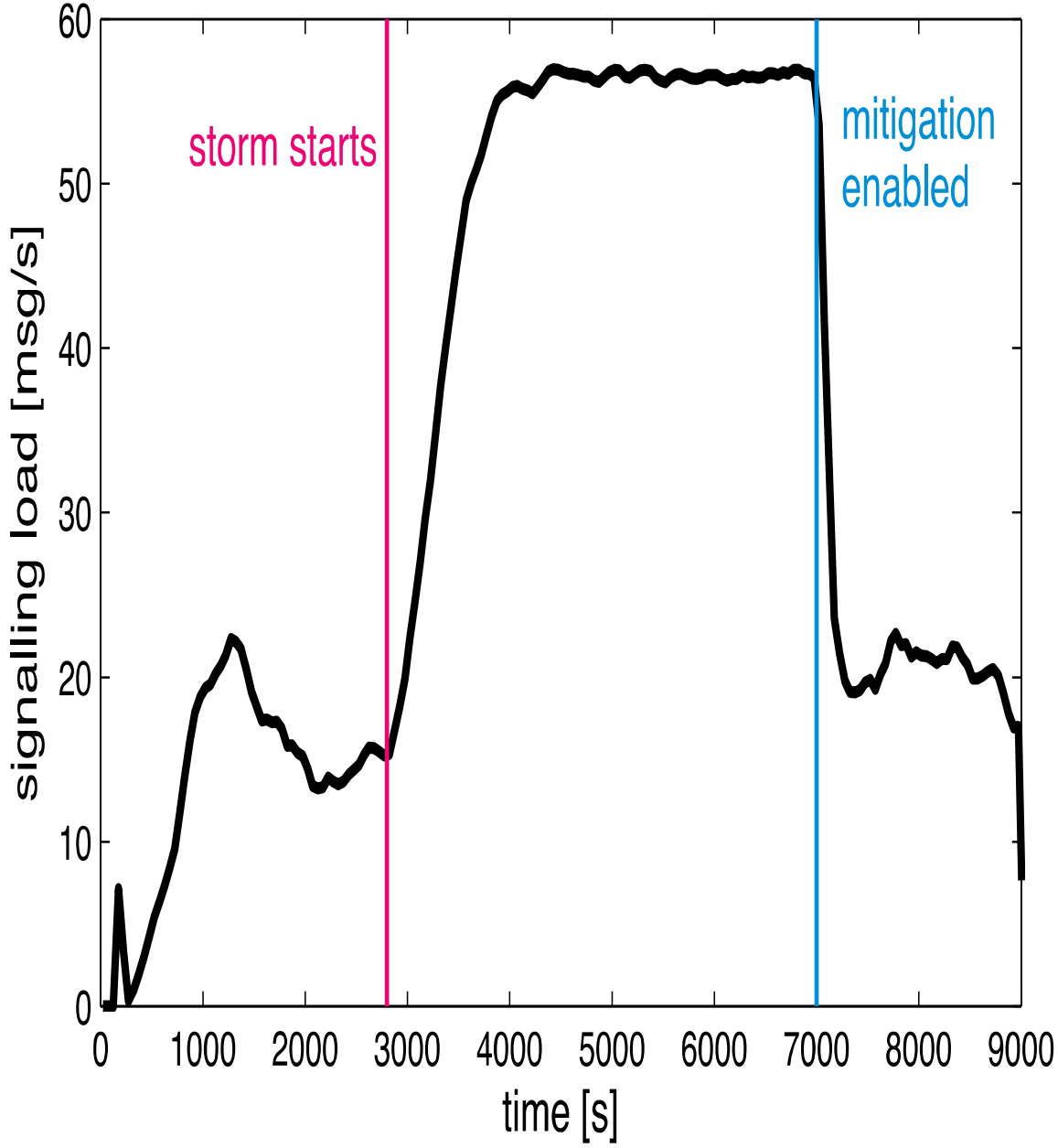
Mobile Network Signalling Attacks

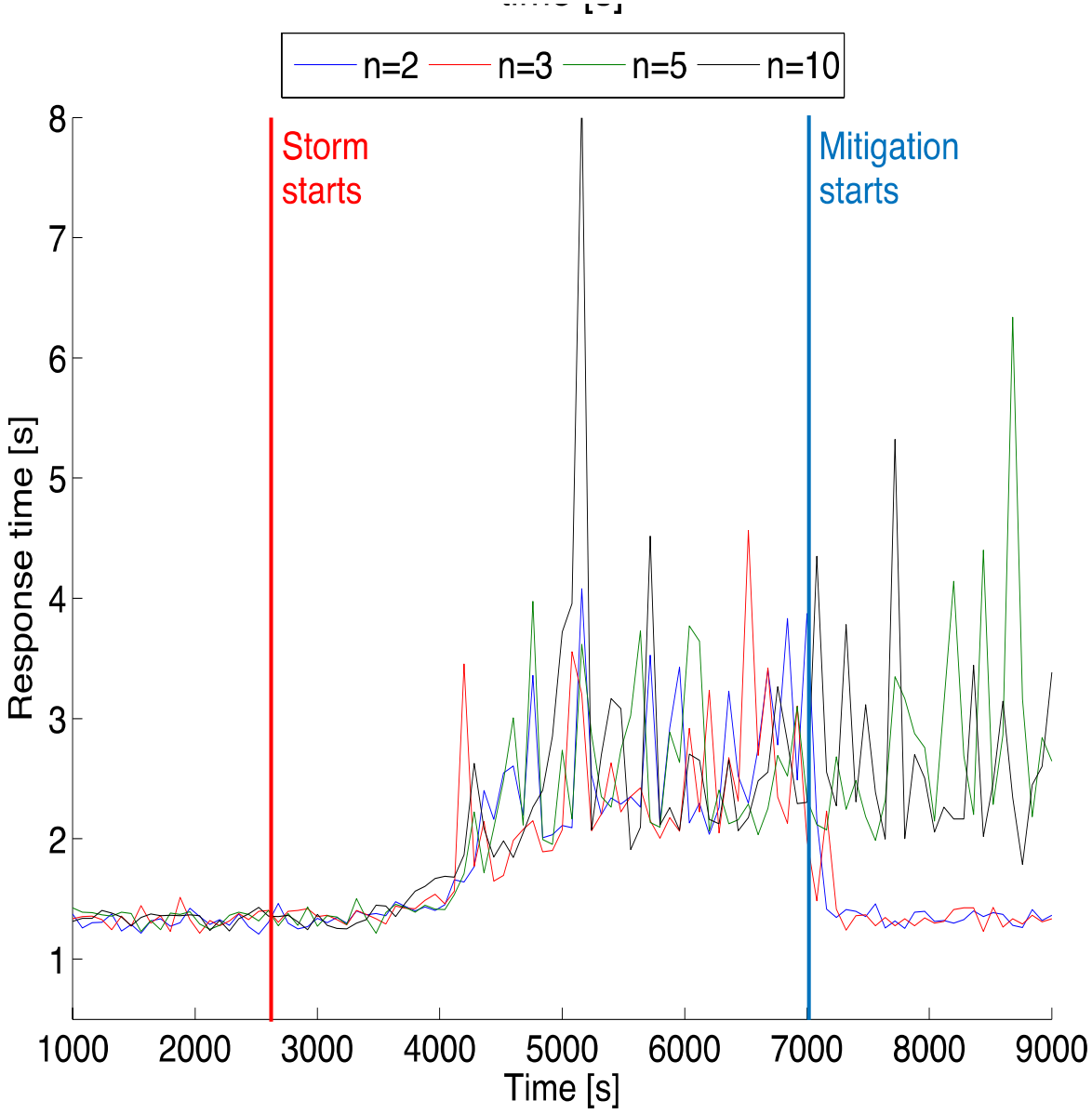

1-p^r_{10}
Cell 1
λ^r_{01}
μ_b
λ^r_1
Signaling server
λ^r_s
μ_s
Cell 1
γ^r_1
Cell N
λ^r_{0N}
μ_b
λ^r_N
p^r_{ib}
Cell N
γ^r_N
$(1\text{-}p^r_{b0})\, p^r_{ij}$
p^r_{b0}
p^r_{i0}
Signaling stage
Communication stage


Normal calls - simulation
Attack calls - simulation
Normal calls - model
Attack calls - model
Average number of calls in service [call]
Attack arrival rate λ^a_0 [call/s]
0
5
10
15
20
0
10
20
30
40
50

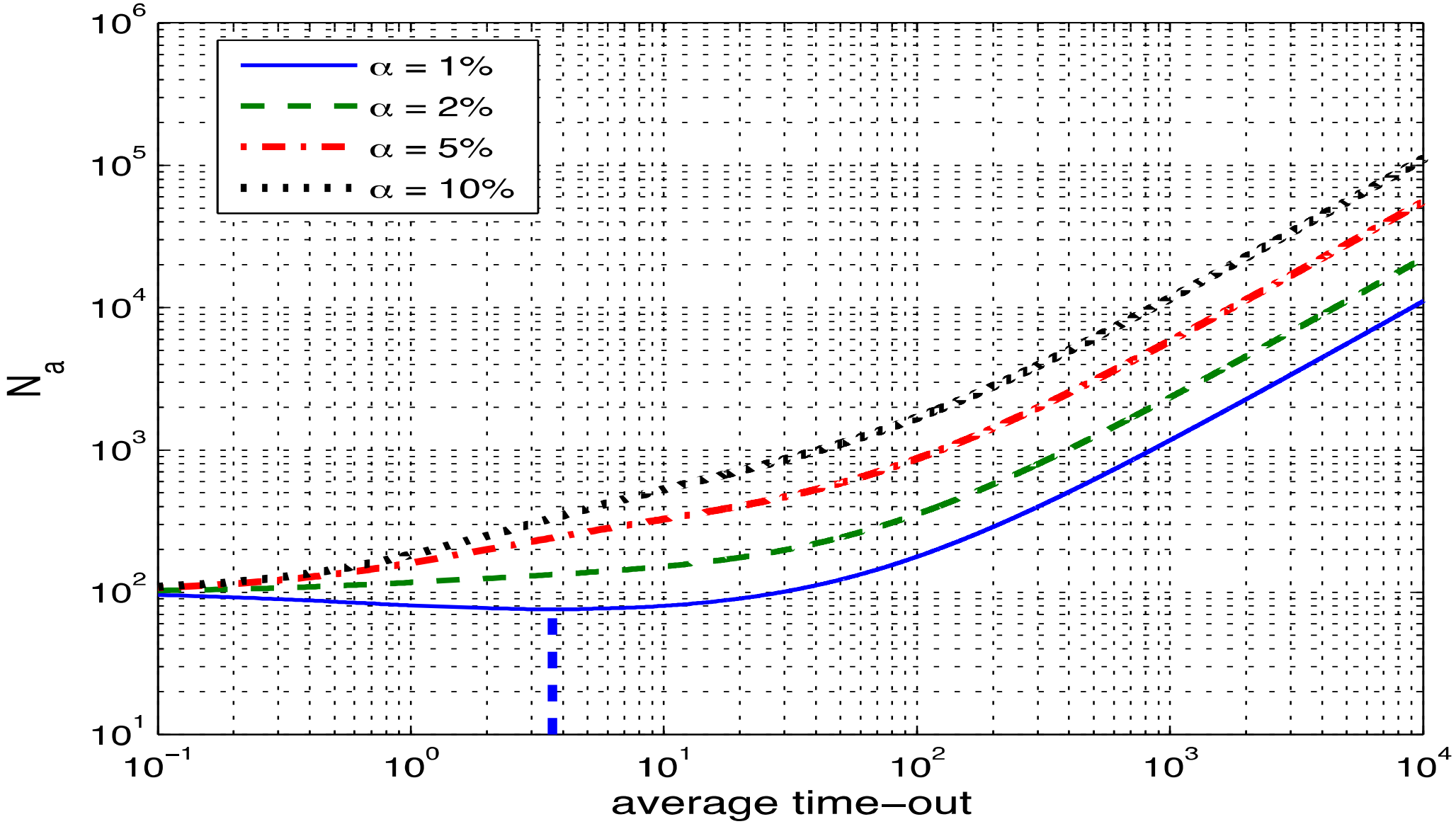

Simulation
Model
Signaling delay [ms]
Attack arrival rate λ^a_0 [call/s]
8
10
12
14
16
18
20
22
24
0
10
20
30
40
50

Signalling Attacks and Defense in Mobile Telephones

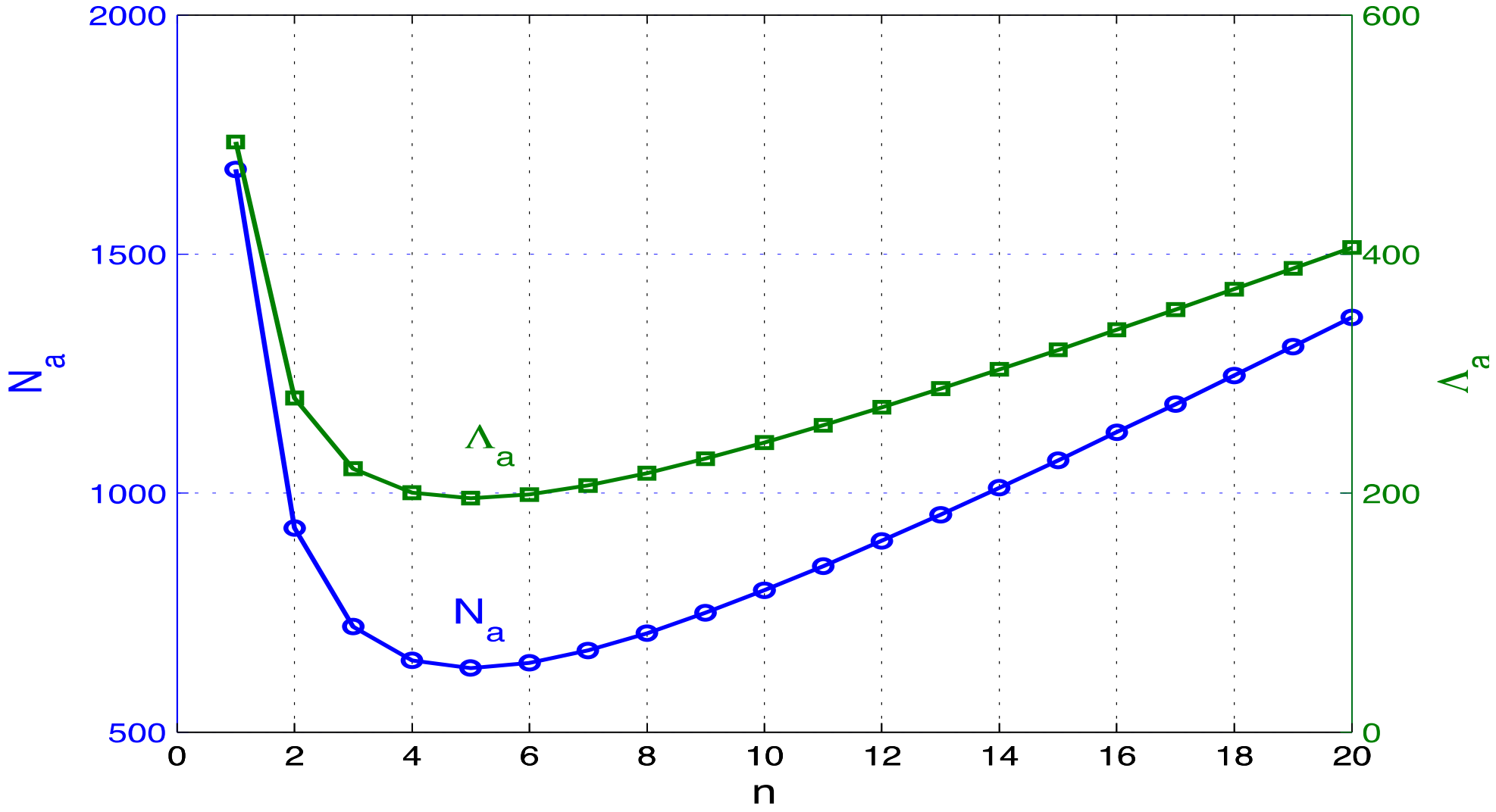




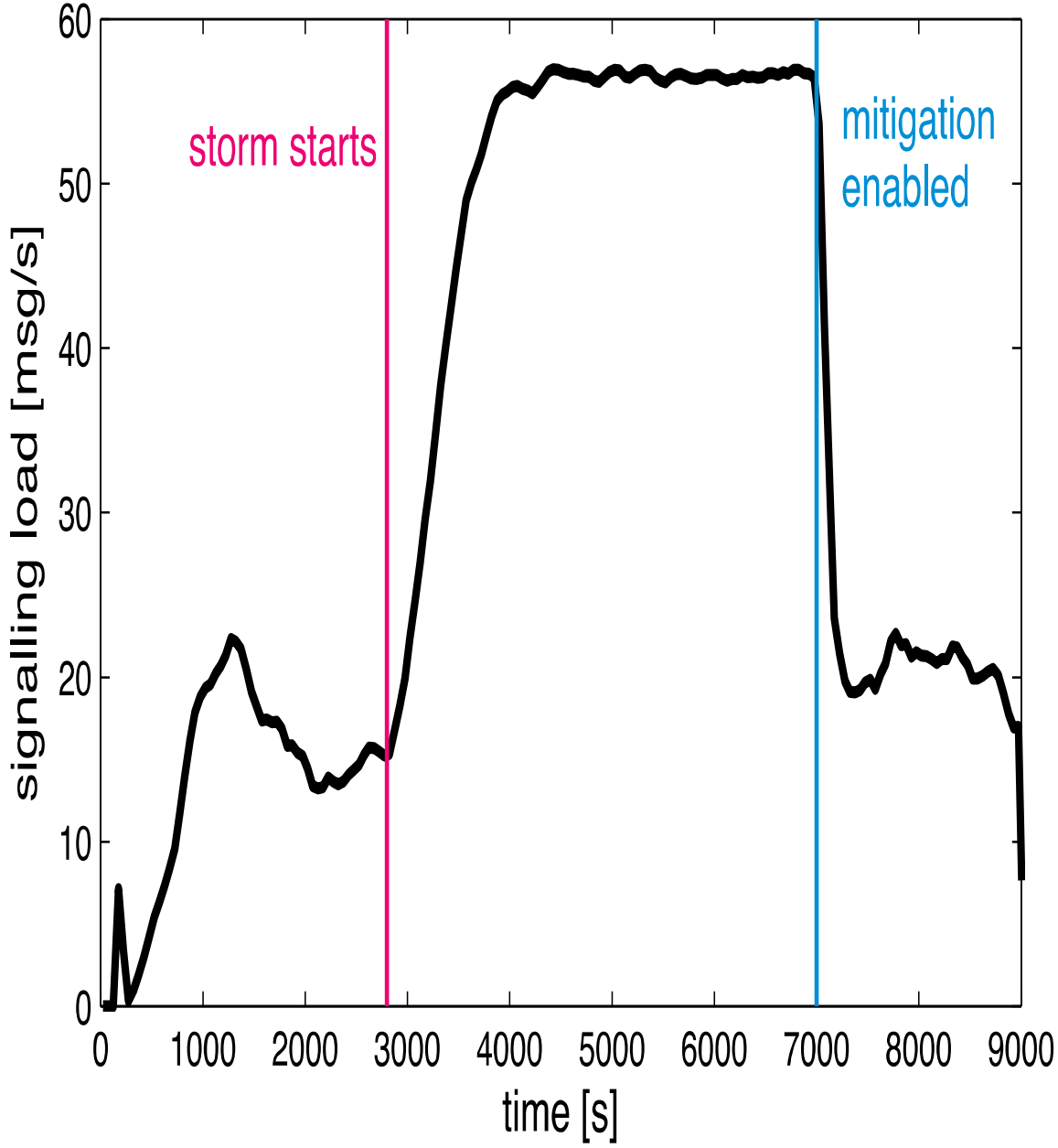
Using the Number of Call Repetions as an Attack Mitigator

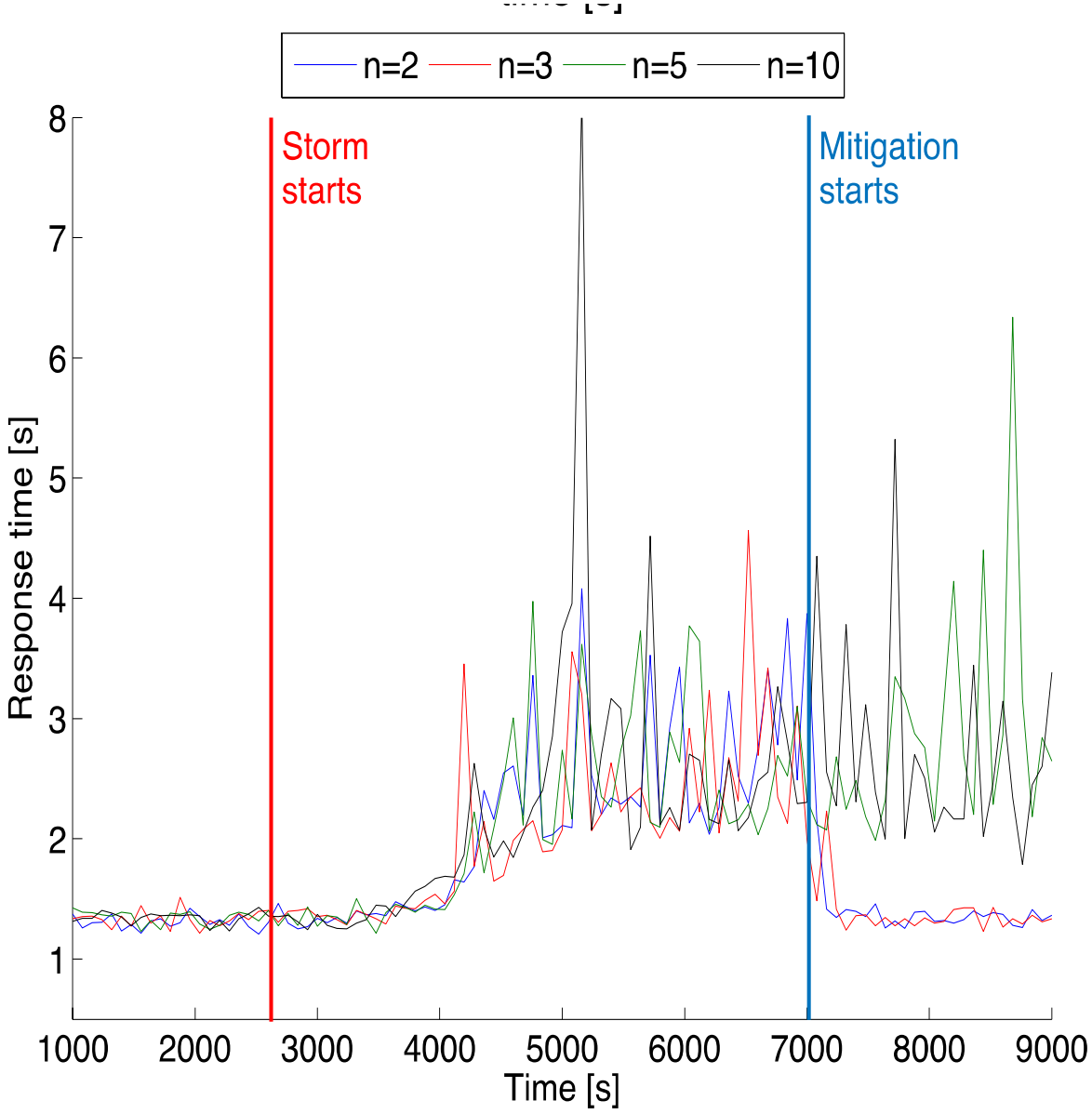


Using the Number of Call Repetitions as an Attack Detector



Signalling Attacks and Defense in Mobile Telephones





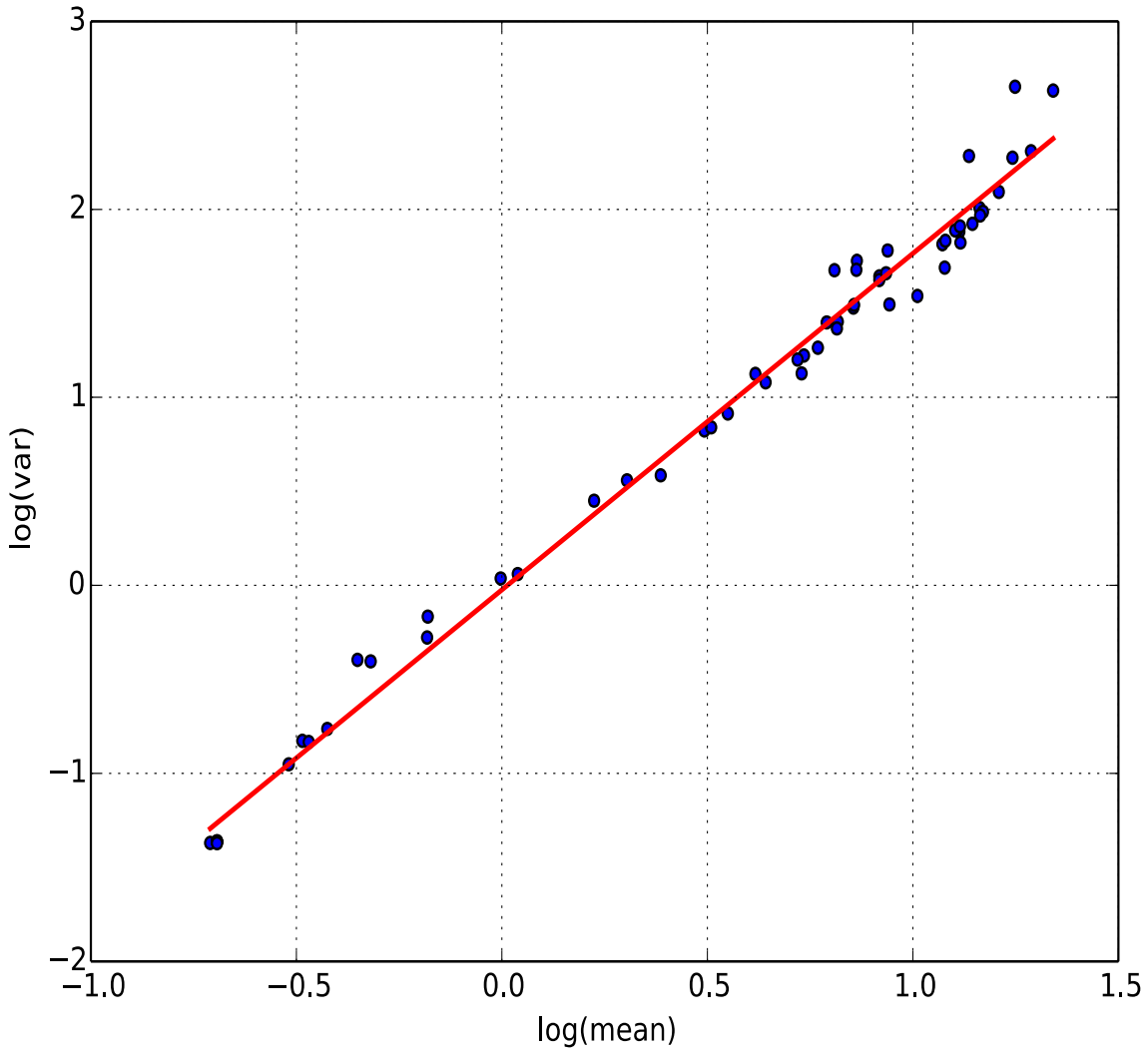
Taylor's "Law" Relates the Average to the Variance of a Random Variable as a Linear Log-Log Relation Its Violation Indicates Potential Attacks

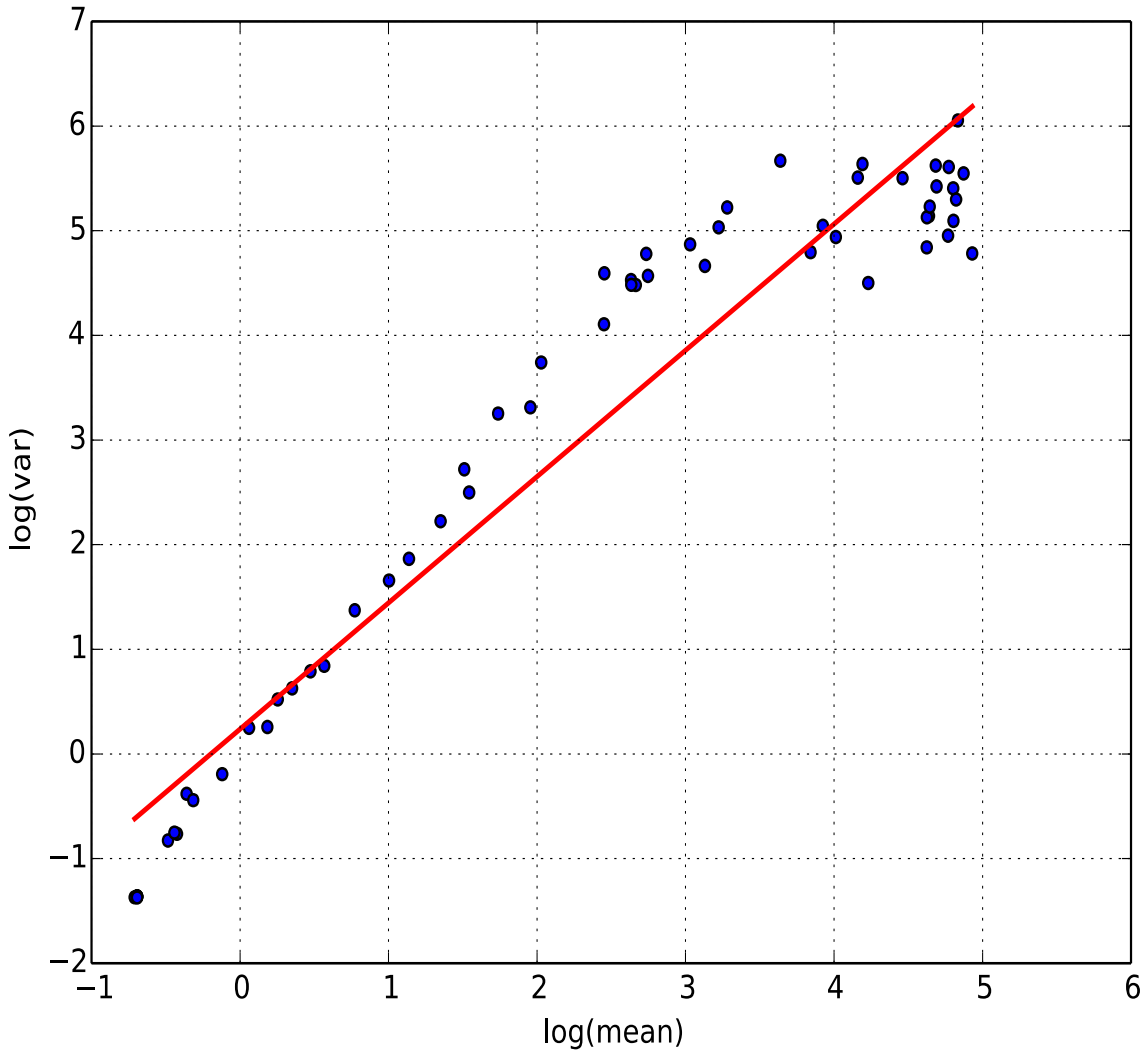
Taylor's Law indicates that we will often empirically observe a linear relationship of the form:

$$A_i = \alpha V_i^{\beta}, \ or \tag{1}$$
$$\log A_i = \log \alpha + \beta \log V_i,$$

where the relation (2) is obviously linear on a $log - log$ scale.

Violation of Taylor's Law as a Sign of Signalling Attacks

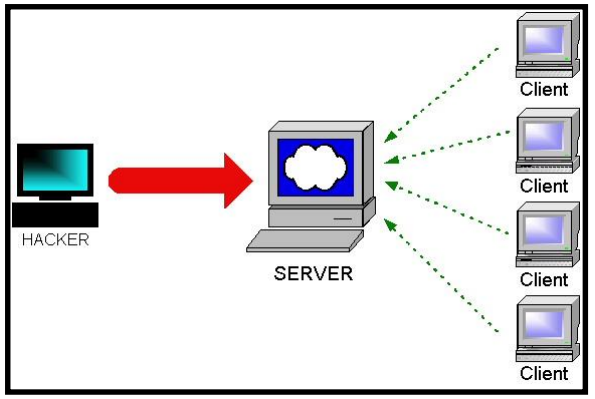


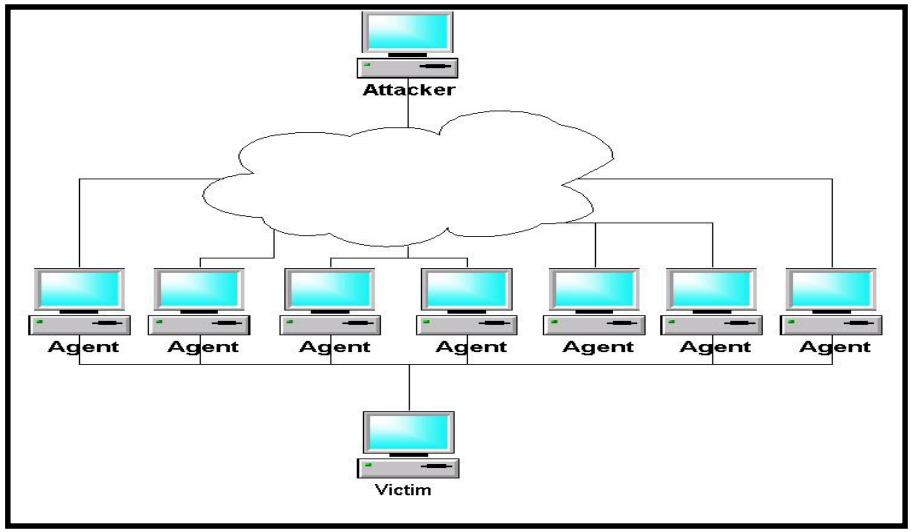


Using Taylor's Law as an Attack Detector: Low (Left) High (Right)

What is a CyberAttack?

A set of Internet and Server based Actions, including the sending of data traffic to one or more servers, with the purpose of preventing legitimate users from using Specific System Resources, or Overloading a System Resource, or aiming at Exploiting the legitimate Users' use of the resource for a third party (attacker's) benefit.



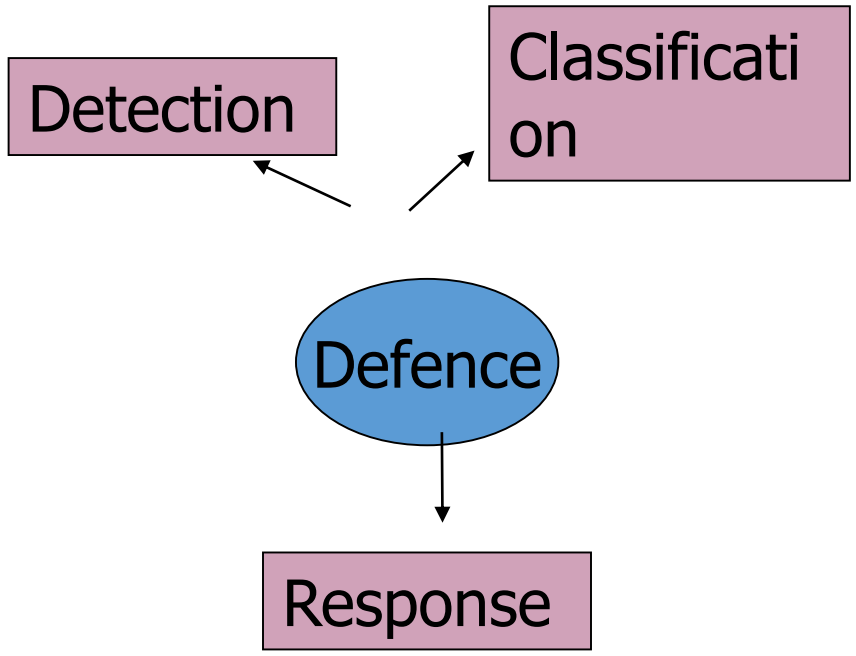


Defence techniques

(signatured- & anomaly-based)
Learning techniques
Statistical signal analysis, Wavelet transform analysis,
Multiple Agents
Fuzzy …

Passive tests
- Loyal clients (beyond suspicion)
- Hop-count filtering (check the TTL) …

Active tests: CAPTCHAs; Cryptographic puzzles



Proactive server roaming
Pushback
Secure overlay tunneling
Dynamic resource pricing

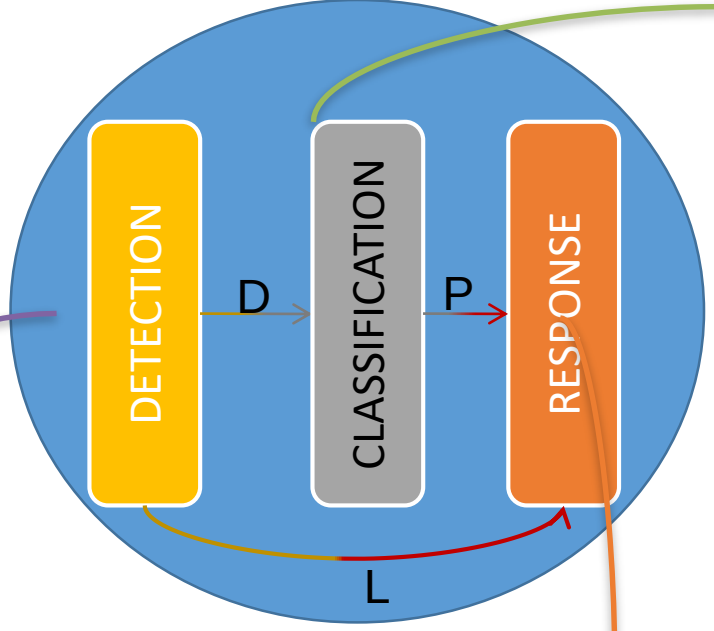
Attack Detection
A numerical value for the overall attack likelihood is going to be calculated which will trigger prioritisation and rate-limiting mechanisms

↓

Classification
by prioritisation

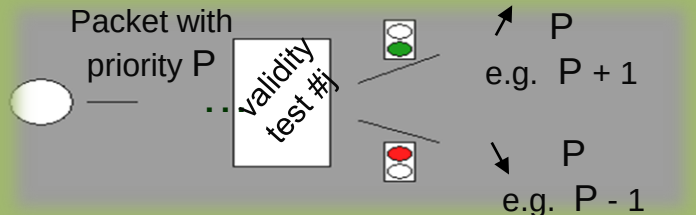
↓

Response by rate-limiting
The ratio of the packets to be dropped will be determined by the numerical value of the attack likelihood calculated during attack detection

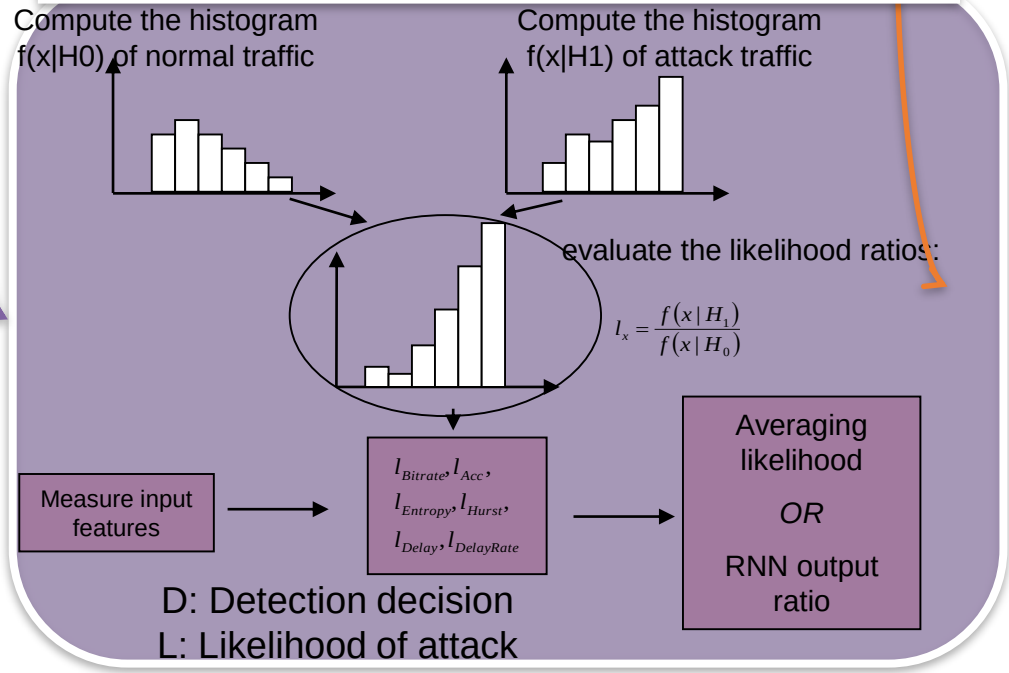


VALIDITY TESTS

- Loyalty of client
- Time of arrival of flow
- Bitrate of flow
- ...



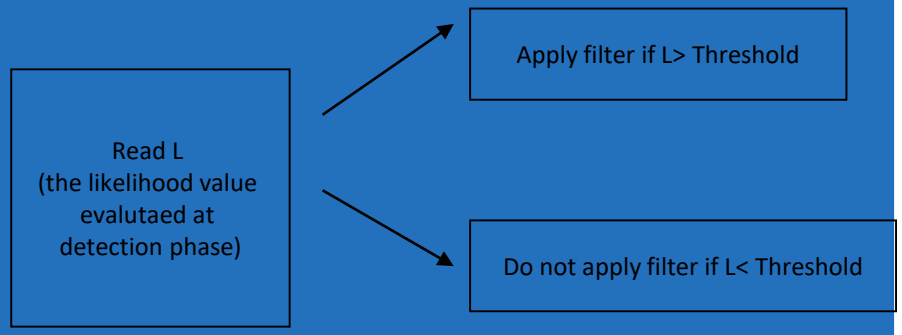
MAXIMUM LIKELIHOOD OR RNN DETECTION



PRIORITISATION

RATE-LIMITING

REROUTING



DDoS Attack Detection Using Bayesian Classifiers & Random Neural Networks

Select the Input Features

- Total incoming bit rate
- Change in total incoming bit rate (acceleration)
- Entropy
- Hurst Parameter
- Delay
- Delay Rate

Gather statistical information on DoS and normal traffic

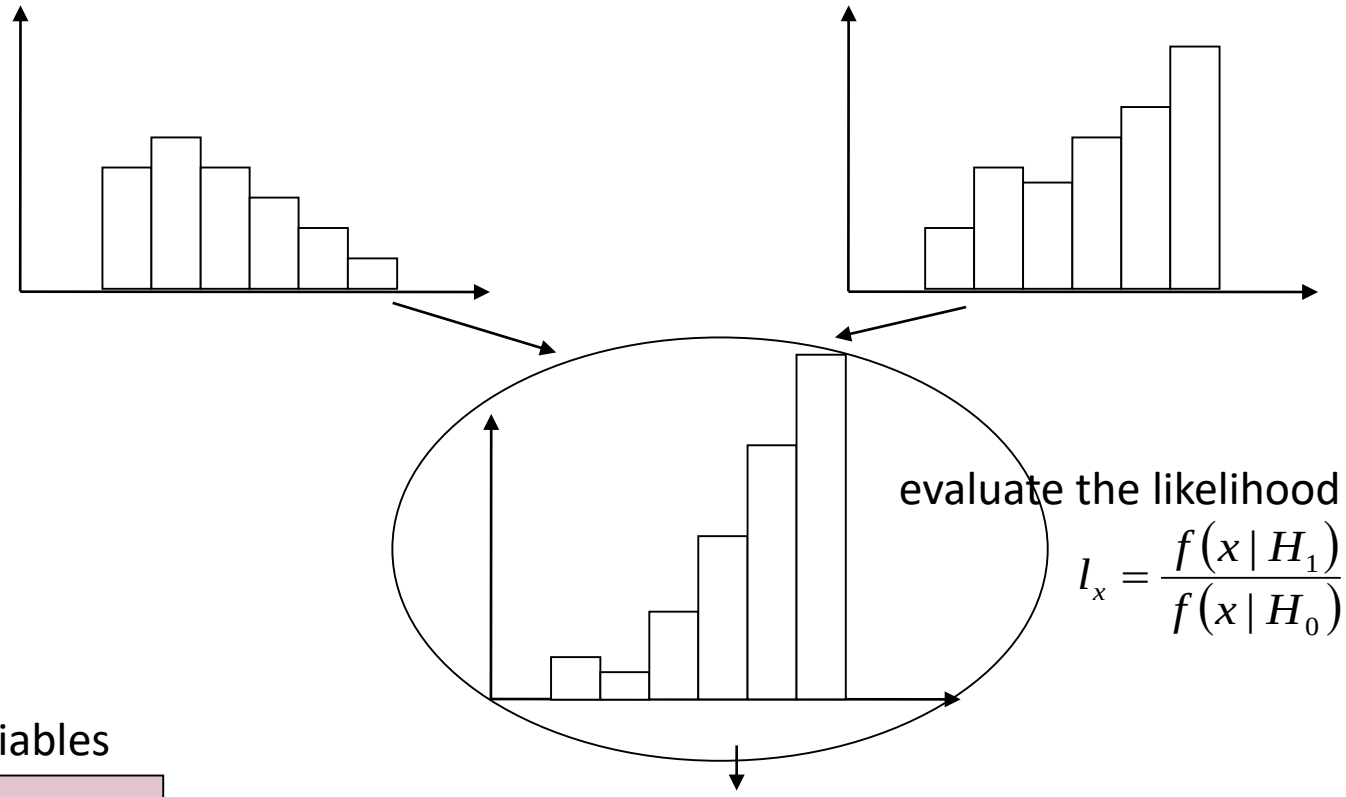
- Obtain histograms
- Evaluate likelihood ratios
- Set thresholds

Real-time decision taking

- Measure the real-time values of the input features from the actual traffic
- Detect Attacks
- Rate Limit Attack Traffic, Re-Route Valid End-User Traffic

Compute the histogram
f(x|H0) of normal traffic

Compute the histogram
f(x|H1) of attack traffic



evaluate the likelihood ratios:

$$l_x = \frac{f(x \mid H_1)}{f(x \mid H_0)}$$

Decision Variables

- Bit rate
- Change in bit rate (acc)
- Entropy
- Self-similarity (Hurst)
- Delay
- Delay Rate

$$l_{Bitrate}, l_{Acc},$$
$$l_{Entropy}, l_{Hurst},$$
$$l_{Delay}, l_{DelayRate}$$

Averaging likelihood OR

RNN

Randomness

Entropy $$S = -\sum_{i=1}^{n} f_i \log_2 f_i$$

Self-Similarity

The Hurst Parameter represents the degree of self-similarity.

We have used the *R/S* statistic to calculate the Hurst parameter

x : **incoming bit rate**

$$(R/S)_N = \frac{1}{s_N}\left[\max_{1\le n\le N}\sum_{n=1}^{N}\left(x-\bar{x}\right)-\min_{1\le n\le N}\sum_{n=1}^{N}\left(x-\bar{x}\right)\right]$$

$$s_N = \left[\frac{1}{N}\sum_{n=1}^{N}\left(x-\bar{x}\right)^2\right]^{1/2}$$

$$(R/S)_N = cN^H$$

Random Neural Network (RNN)

✓**RNNs represent an approximation of the true functioning of a biophysical neural network, where the signals travel as spikes rather than analog signals**

✓**They are computationally efficient structures.**

✓**They are easy to simulate since each neuron is simply represented by a counter.**

$$\sum_j \left(p^+(i,j) + p^-(i,j)\right) + d(i) = 1$$

$$w^+(j,i) = r(i)\,p^+(i,j) \geq 0$$

$$w^-(j,i) = r(i)\,p^-(i,j) \geq 0$$

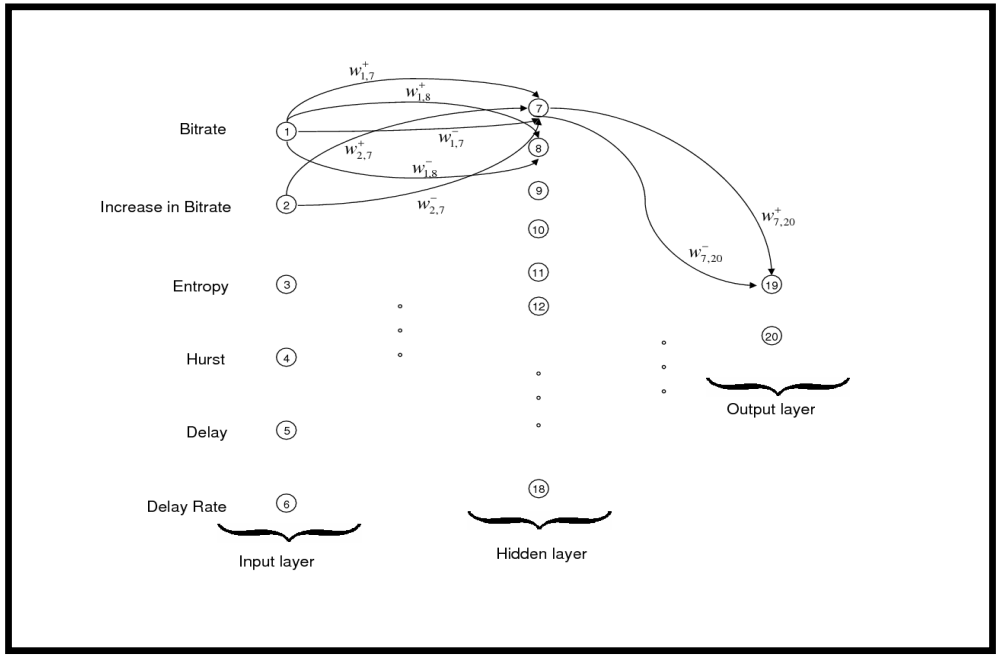
The potential for neuron *i* is:

$$q_i = \frac{N(i)}{D(i)}$$

$$N(i) = \sum_j q_j w^+(j,i) + \Lambda(i)$$

$$D(i) = r(i) + \sum_j q_j w^-(j,i) + \lambda(i)$$

$$r(i) = \sum_j w^+(i,j) + w^-(i,j)$$

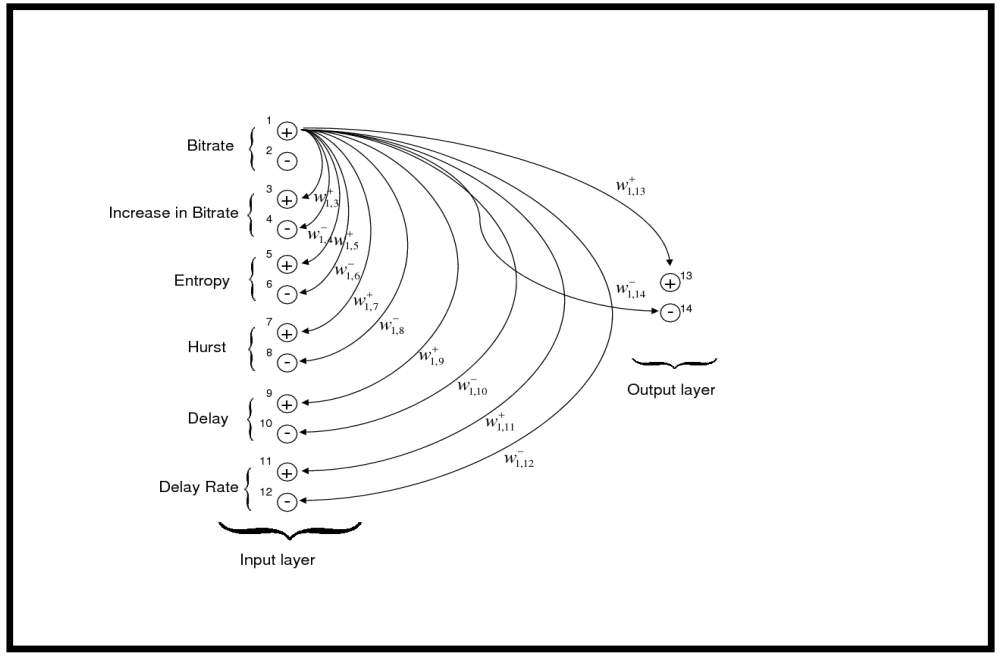


Feedforward RNN

An input layer of six neurons, a hidden layer with twelve neurons and an output layer with two neurons.

Each output neuron stands for a decision; attack or not.

The final decision is determined according to the ratio of the two output neurons.



Recurrent RNN

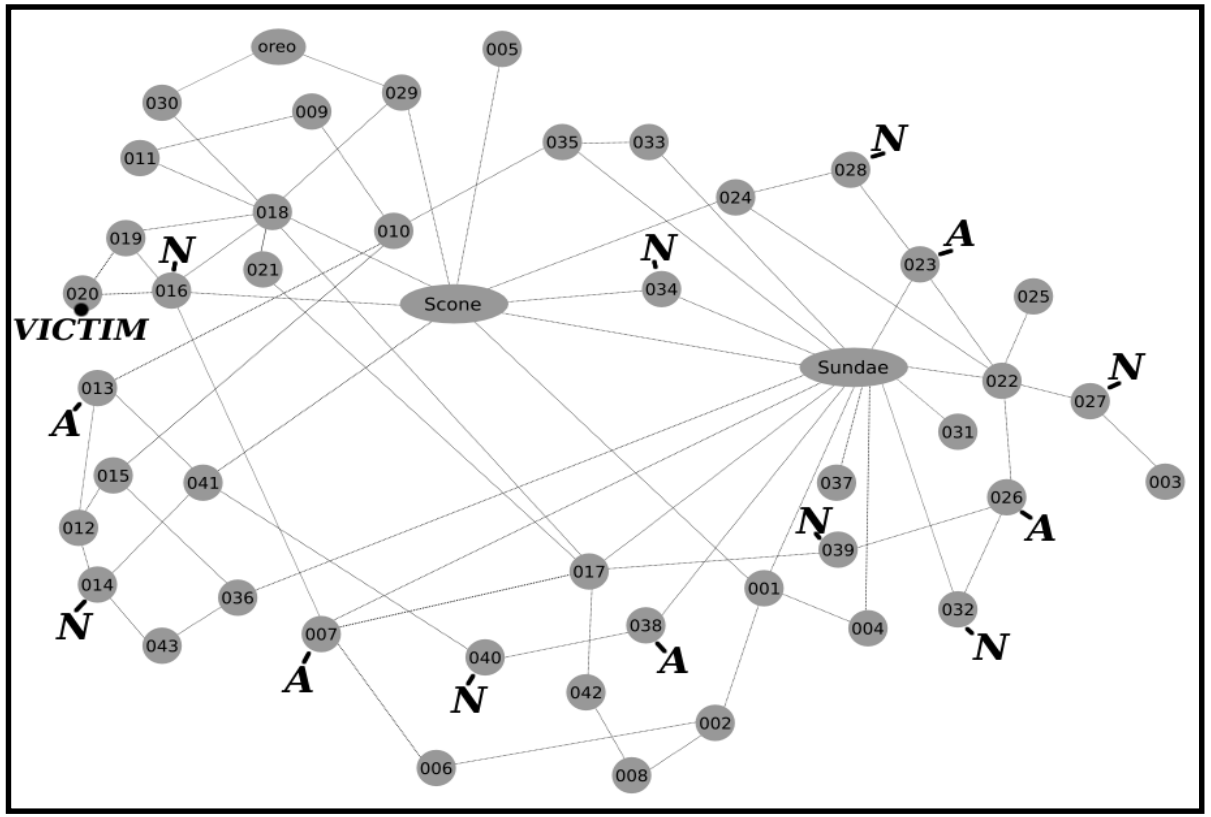
It consists of an input layer with twelve neurons and an output layer with two neurons.

In the input layer, there are two neurons for each input variable; one for the excitatory signals and one for the inhibitory signals.

Each neuron sends excitatory signals to same type of neuron and inhibitory signals to opposite type of neuron.

At the output layer, excitatory signals are collected at one neuron and inhibitory signals are summed up at the second neuron.

Experimental Results



Topology of the test-bed used in the experiments (Node 20 is the victim)

We have used four data sets:

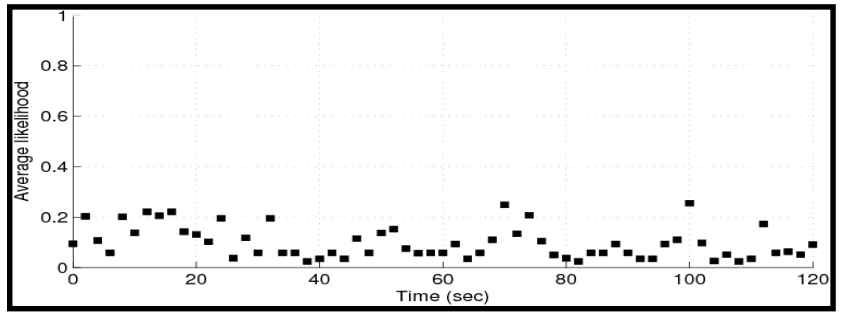
1) Normal traffic

2) Synthetic Attack Traffic

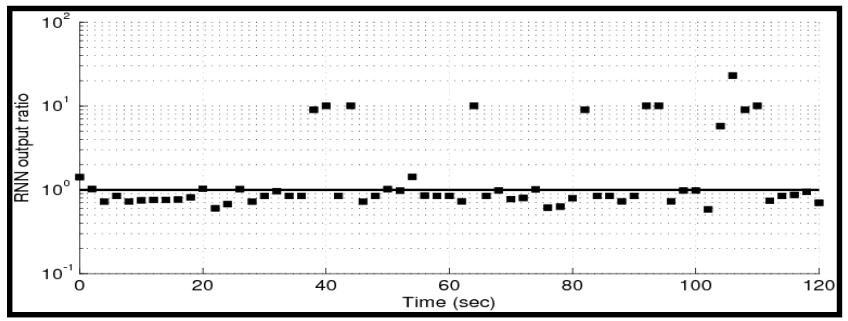
3) Attack traffic extracted from traces downloaded from an online repository (trace1)

4) Attack traffic extracted from traces downloaded from an online repository (trace2)

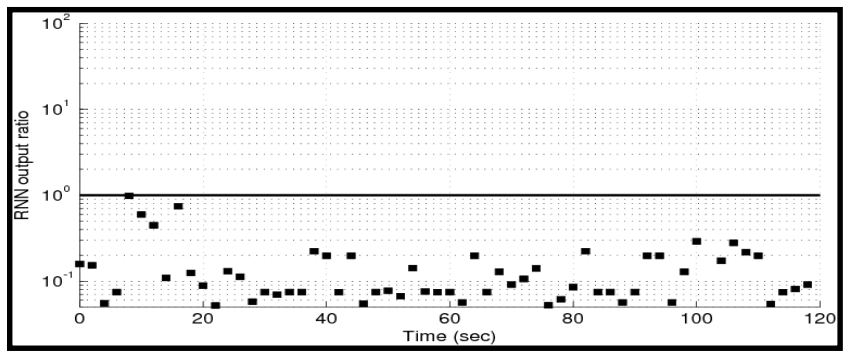
Normal Traffic



Average Likelihood Ratio

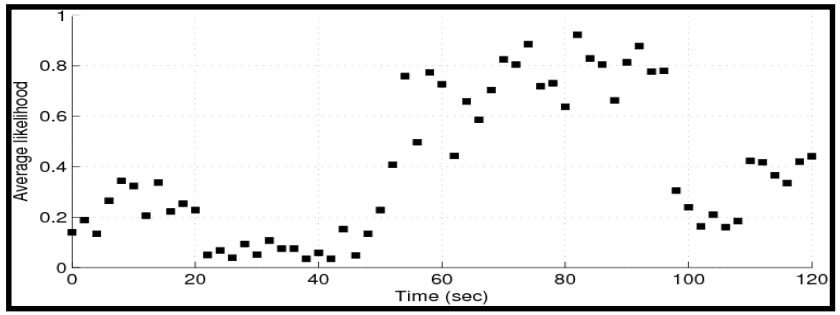


Feedforward RNN



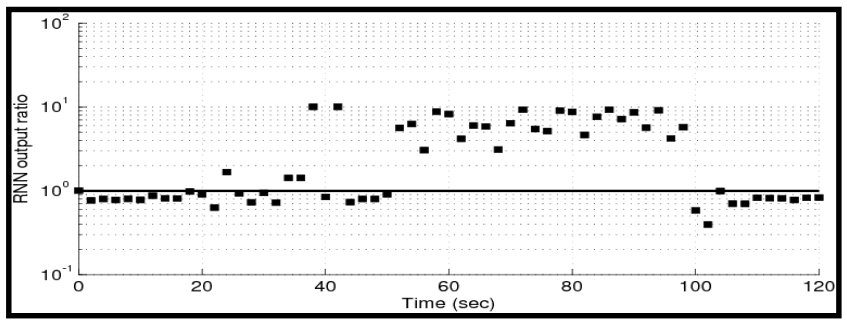
Recurrent RNN

Attack Traffic



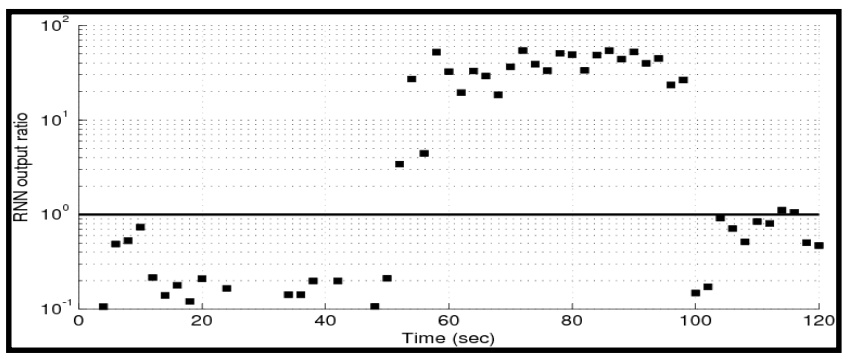
Average Likelihood Ratio

False Alarms: 0 %
Correct Detections: 80 %



Feedforward RNN

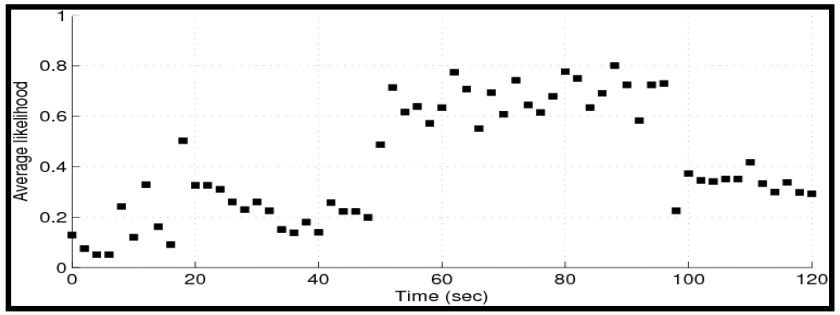
False Alarms: 16.7 %
Correct Detections: 96 %



Recurrent RNN

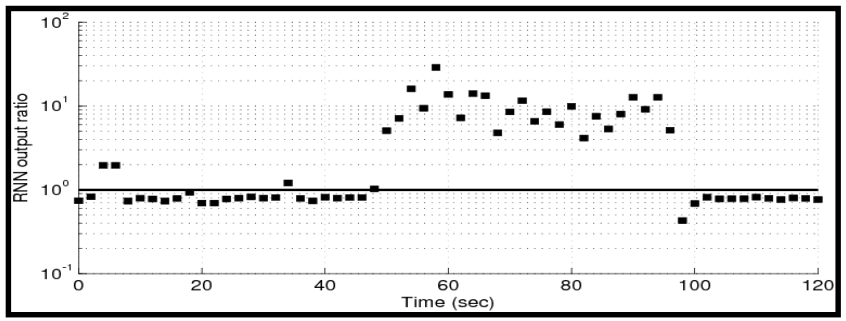
False Alarms: 5.5 %
Correct Detections: 96 %

Trace1 --- Attack Traffic



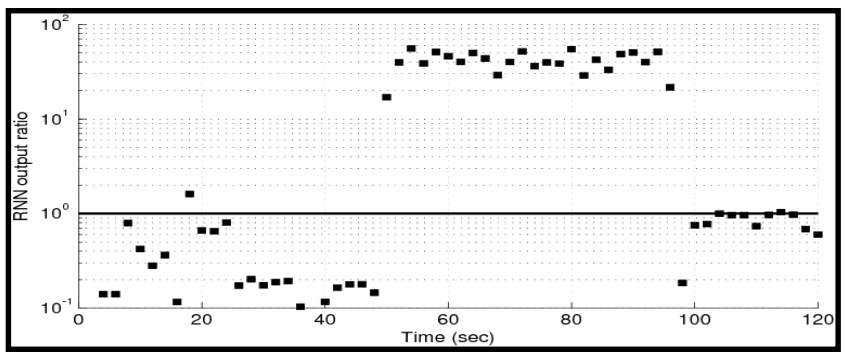
Averaged Likelihood

False Alarms: 2.8 %
Correct Detections: 88 %



Feedforward RNN

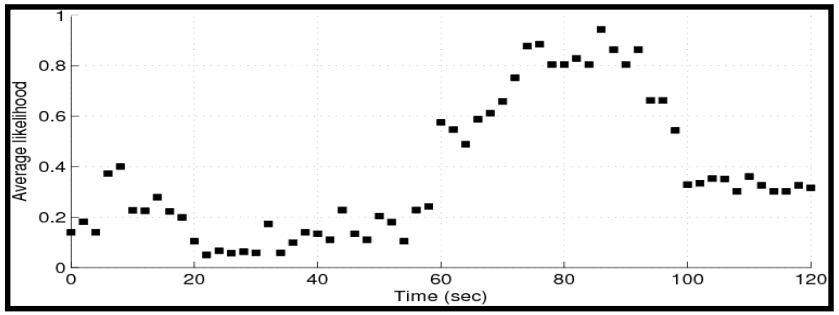
False Alarms: 11 %
Correct Detections: 96 %



Recurrent RNN

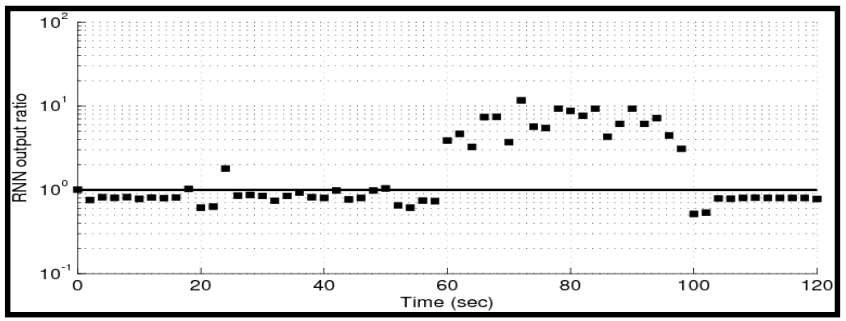
False Alarms: 11 %
Correct Detections: 96 %

Trace2 --- Attack Traffic



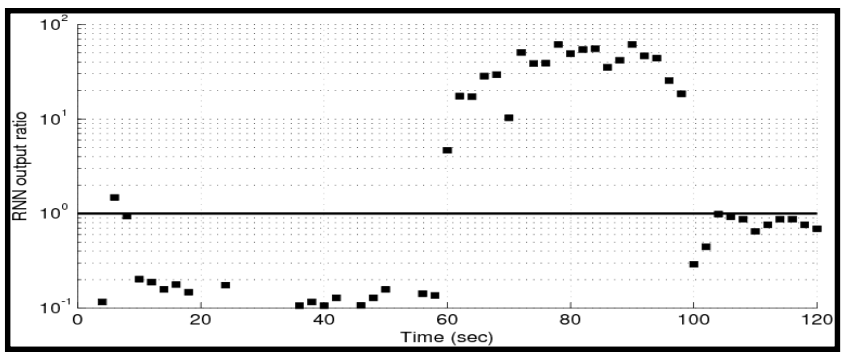
Averaged Likelihood

False Alarms: 0 %
Correct Detections: 76 %



Feedforward RNN

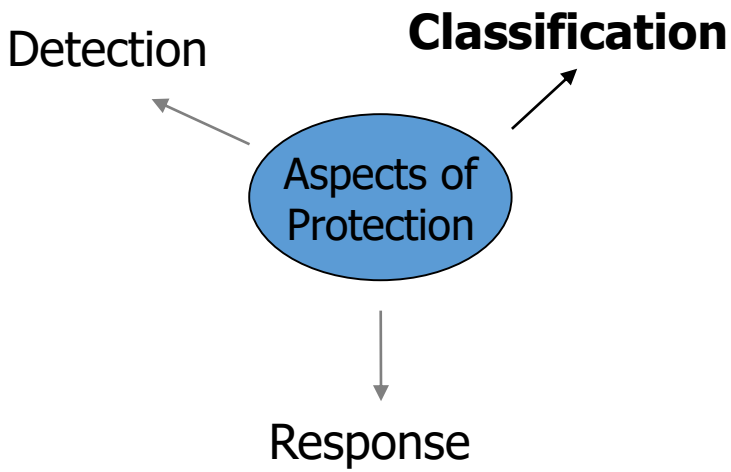
False Alarms: 8.3 %
Correct Detections: 84 %



Recurrent RNN

False Alarms: 2.8 %
Correct Detections: 80 %

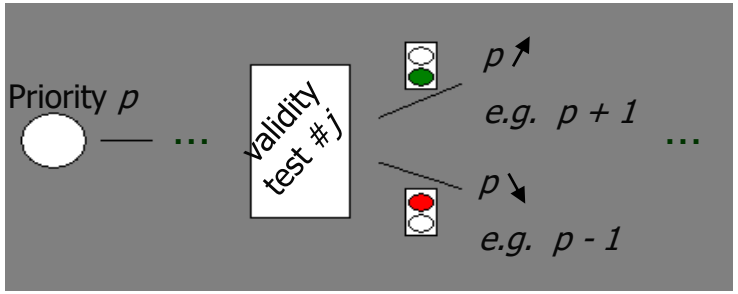
Prioritisation. Traffic prioritisation is a queueing mechanism which serves the packets in strict order of importance (priority). Packets seen as more important (higher priority) receive service always before the ones of the next (lower) priority and so on.



Classification: mark +1 if

- Belongs to list of known sources
- First appearance of source before detection
- Bitrate from source below a threshold

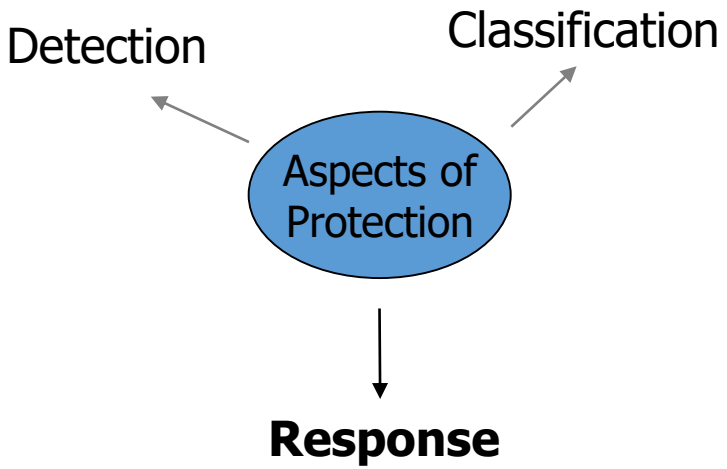
…



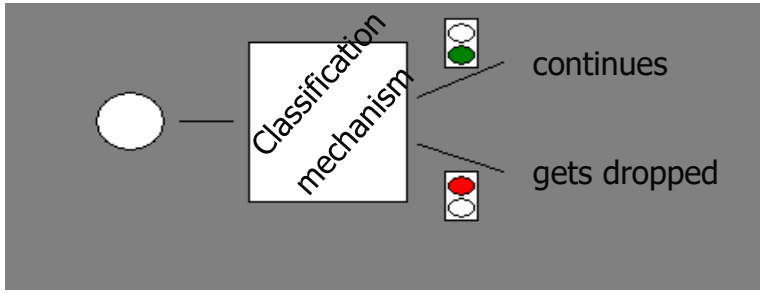
Responding to the attack

- Proactive server roaming
- Pushback
- Secure overlay tunneling
- Dynamic resource pricing

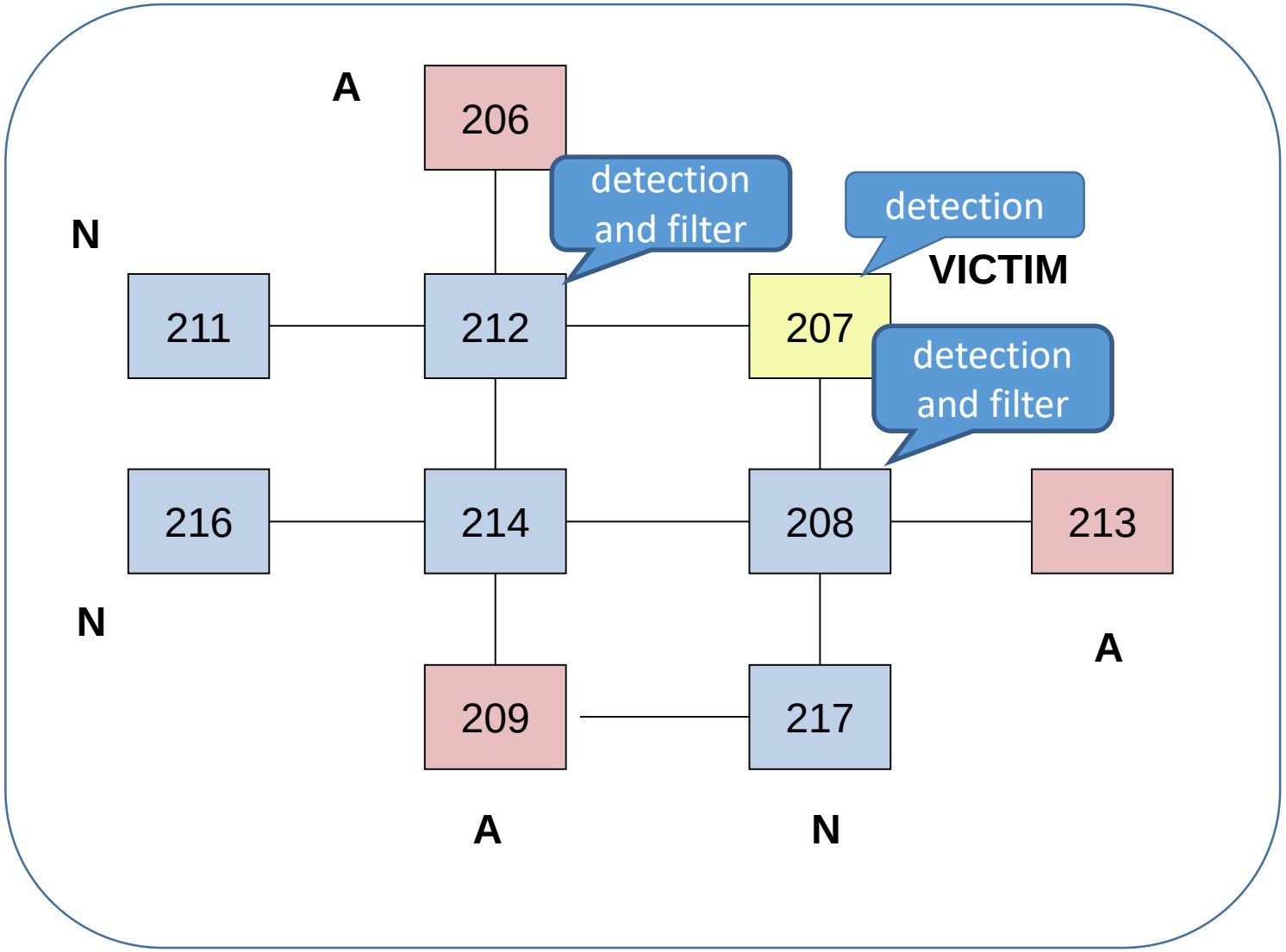
...



Rate-limiting (Throttling). Rate-limiting is the process of allowing traffic only up to a maximum limit to pass. It essentially means that traffic in excess of a set limit is dropped to avoid congestion.

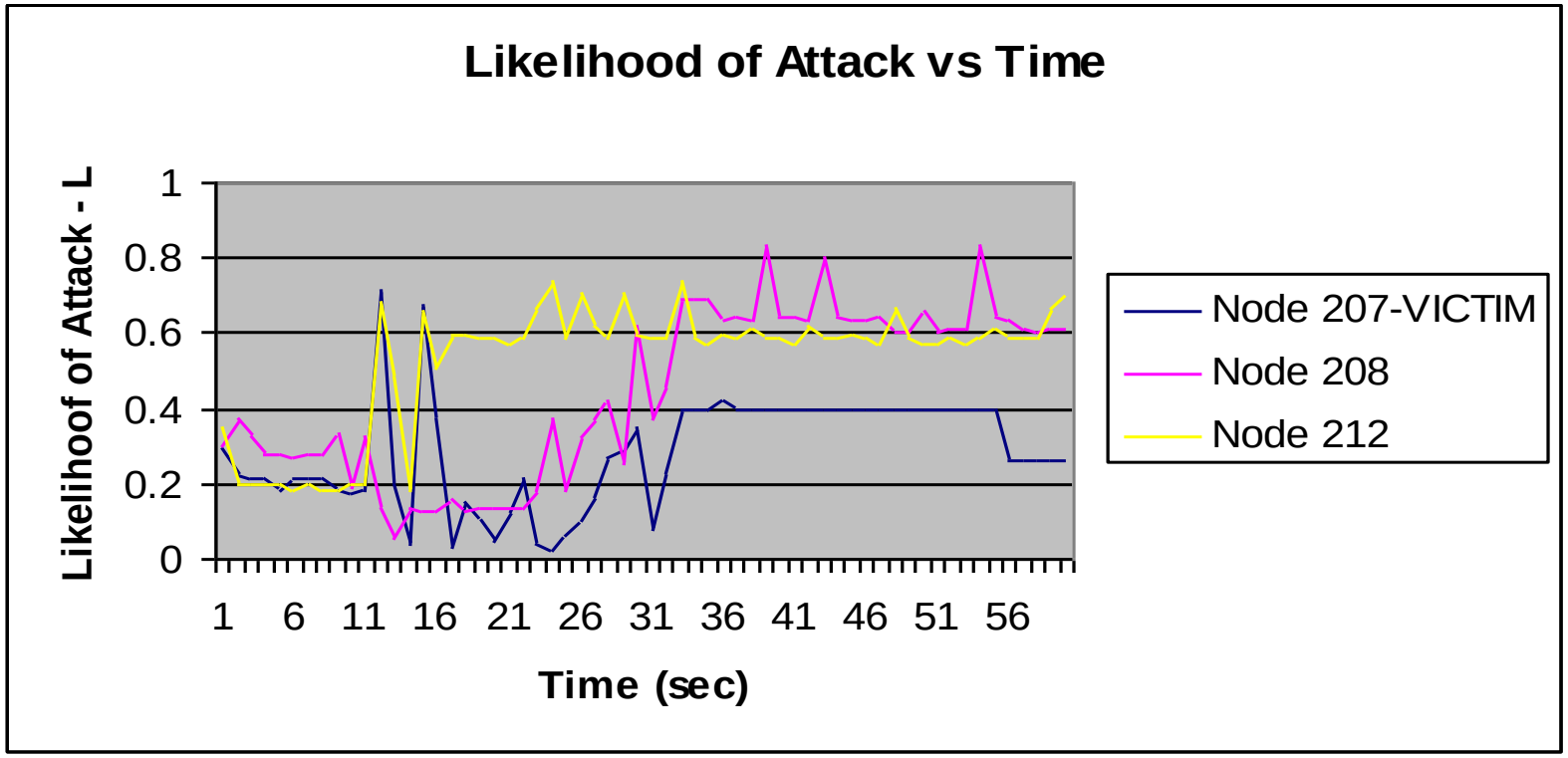


Some Results for Rate-Limiting (By applying a filter)

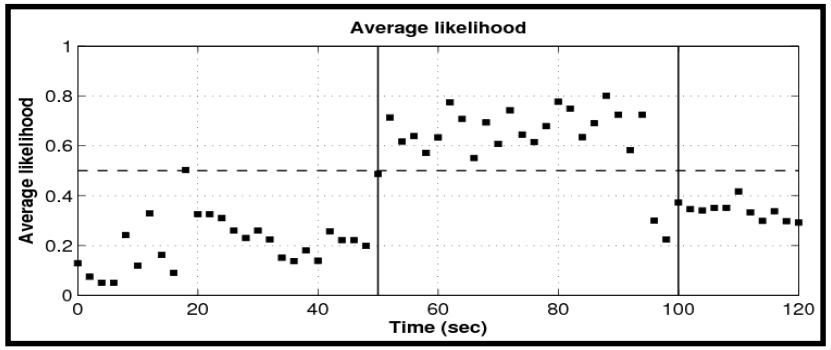


- In our scenario, node 207 is the victim.
- The first hop neighbours 208 and 212 continuously run the detection algorithm and evaluate L(average likelihood of having an attack)
- They compare it with a threshold T.
  If L>T, the filter is applied at the exit of the nodes(208 and 212).
  Thus the bitrate going to 207 is decreased.
- 207 also runs the detection algorithm for justification (L observed should be low now tat the bitrate coming is low).
- It is observed that both at 208 and 212, the incoming bitrate and evaluated likelihood are high.
- In 207 both incoming bitrate and evaluated likelihood are low, due to the filters applied at the first hop neighbours.
- Thus this is a distributed method, where each node detects by itself and decides to apply filter or not.

Experimental Results:

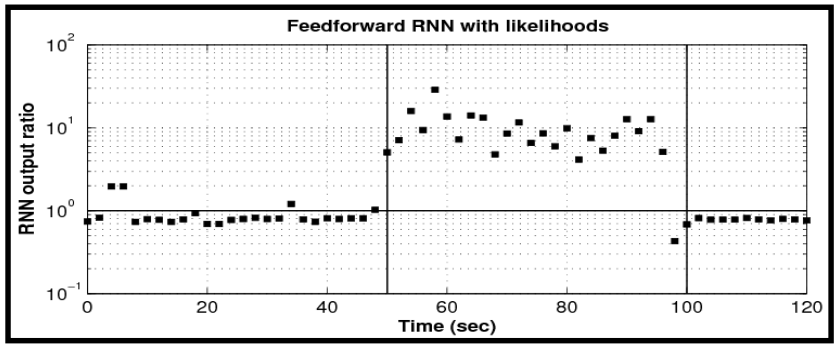


Trace1 --- Attack Traffic



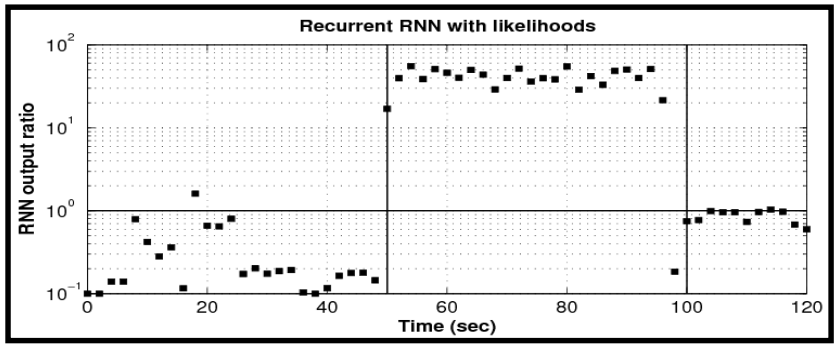
Averaged Likelihood

False Alarms: 2.8 %
Correct Detections: 88 %



Feedforward RNN

False Alarms: 11 %
Correct Detections: 96 %



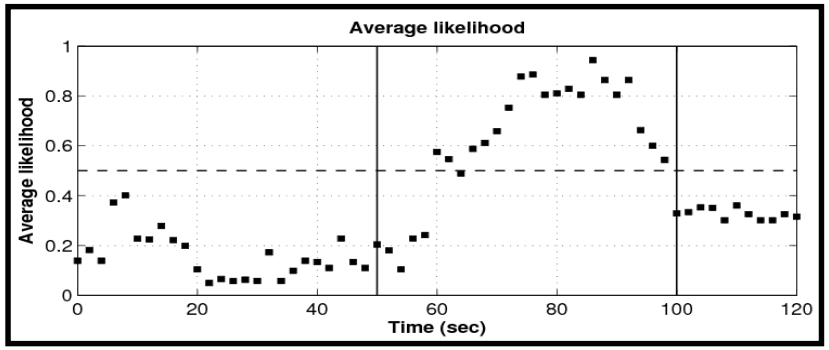
Recurrent RNN

False Alarms: 11 %
Correct Detections: 96 %

Intelligent Systems & Networks

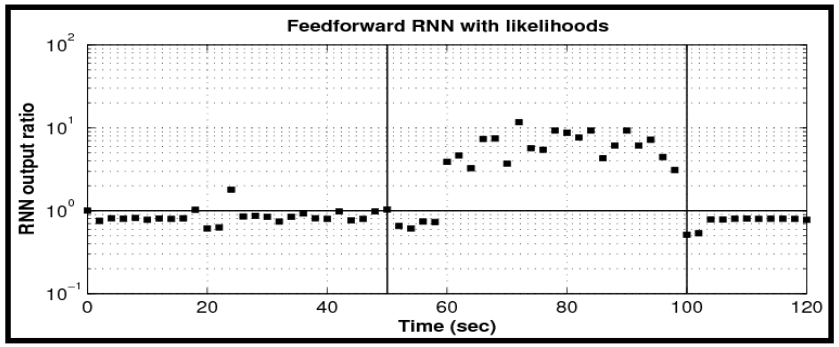
Imperial College London

Trace2 --- Attack Traffic



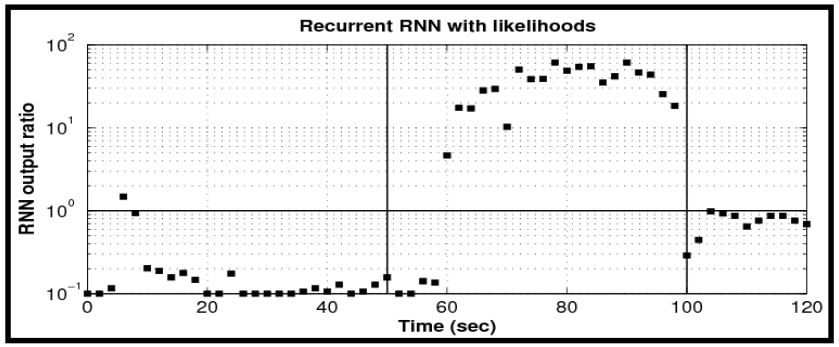
Averaged Likelihood

False Alarms: 0 %
Correct Detections: 76 %



Feedforward RNN

False Alarms: 8.3 %
Correct Detections: 84 %



Recurrent RNN

False Alarms: 2.8 %
Correct Detections: 80 %

Intelligent Systems & Networks

Imperial College London

Battery and Energy Attacks on the IoT

Energy Attacks Through Traffic & Electromagnetic Noise

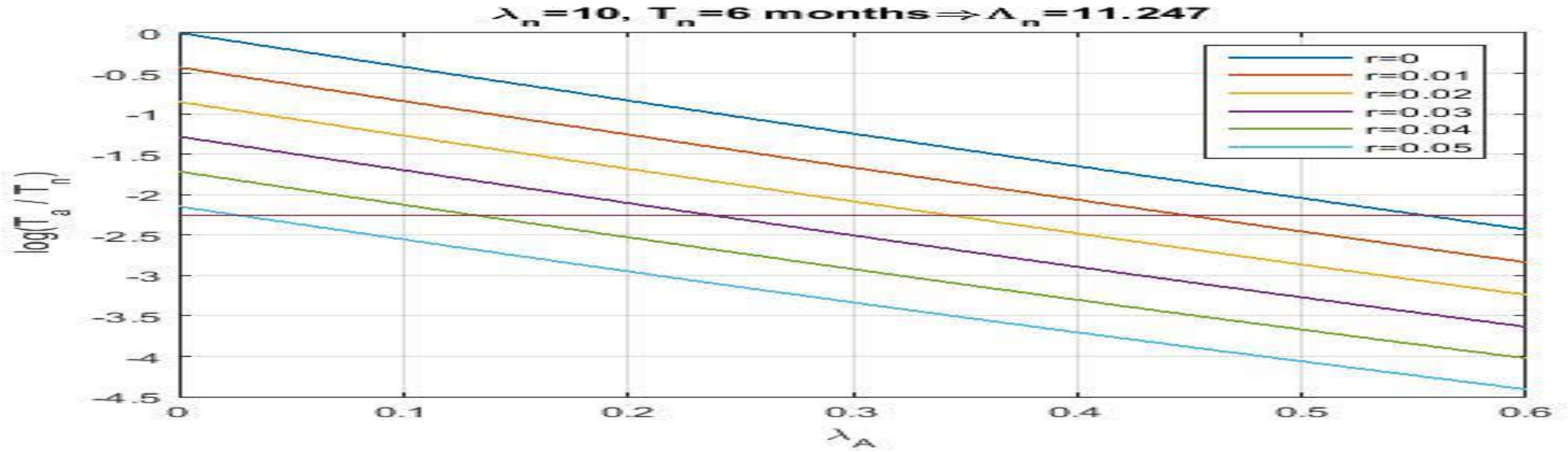


Fig. 1: The curves illustrate the effect of two simultaneous types of attacks, namely the attacks that create added traffic, and those that create retransmissions due to noise that is generated by electromagnetic attacks. We show the variation of the *base 10 logarithm* of the ratio of node energy lifetime under attack, to energy life-time without attacks (y-axis), against the arrival rate of attack traffic λ_A with distinct curves for increasing values of the retransmission probability r due to electromagnetic attacks. The parameter settings are $E = B = 100$, $\gamma = 0.01\Lambda_n$ and $\mu = 0.01\lambda_n$. We fix the "normal life-time" of the system until the battery is emptied after $T_n = 6$ *months* of operation, on average. Thus the EP arrival rate Λ_n representing the required energy harvesting will vary with the normal traffic rate λ_n as shown on each of the graphs. The effect of the attacks is shown by the rapid decrease of the ratio $\log \frac{T_a}{T_n}$ as both λ_A and r increase.

Effect of Battery Size in an Energy Harvesting System on the Energy Life-Time in the Presence of Attacks

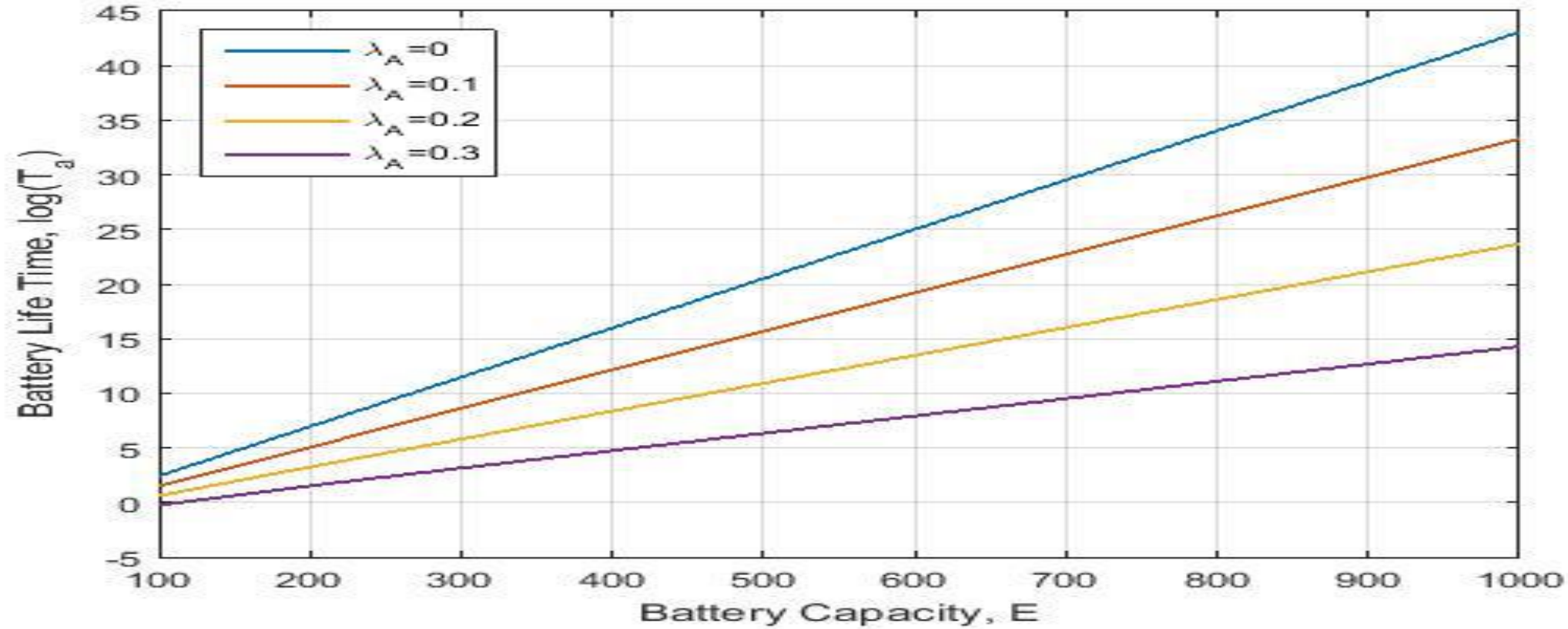


Fig. 3: For a node that uses energy harvesting, its energy life-time is shown on the y-axis versus the local battery capacity E, for three different values of attack traffic and $r = 0.1$. The capacity of the local battery which stores the harvested energy substantially increases the system's energy life-time.

Fixed Battery Size versus Harvesting on Energy Life-Time in the Presence of Attacks

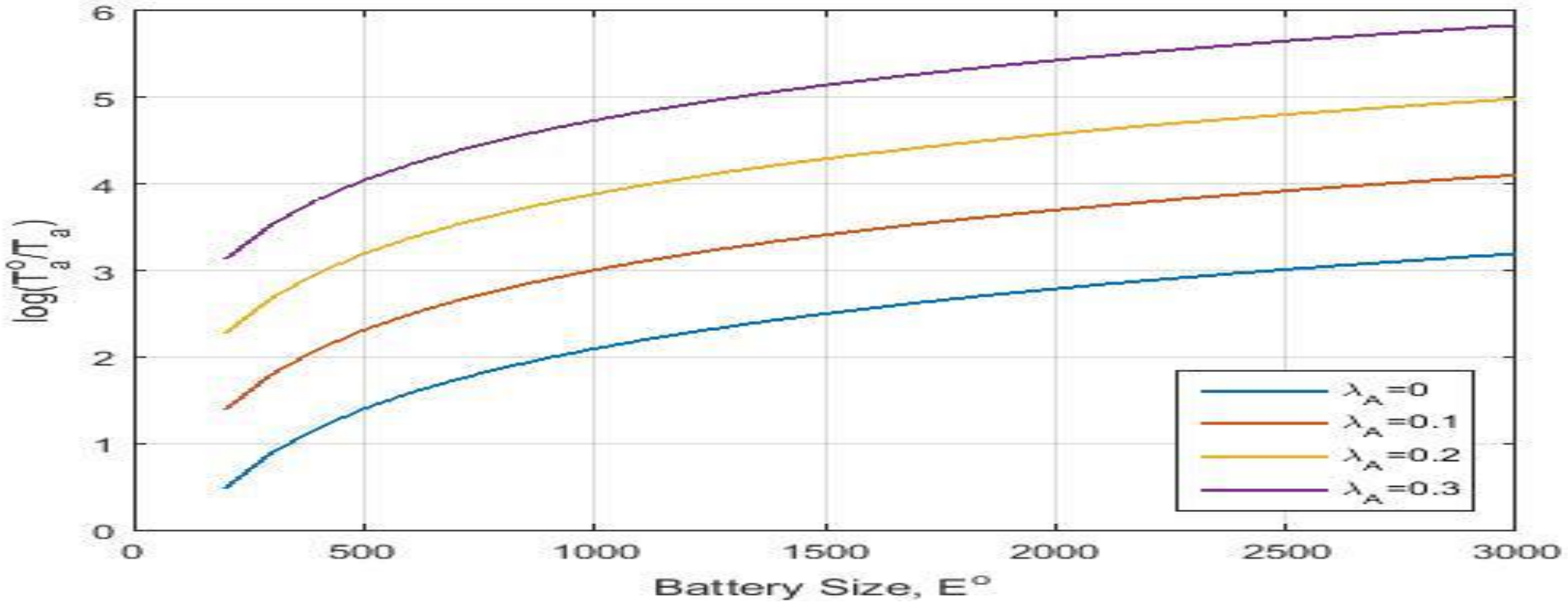
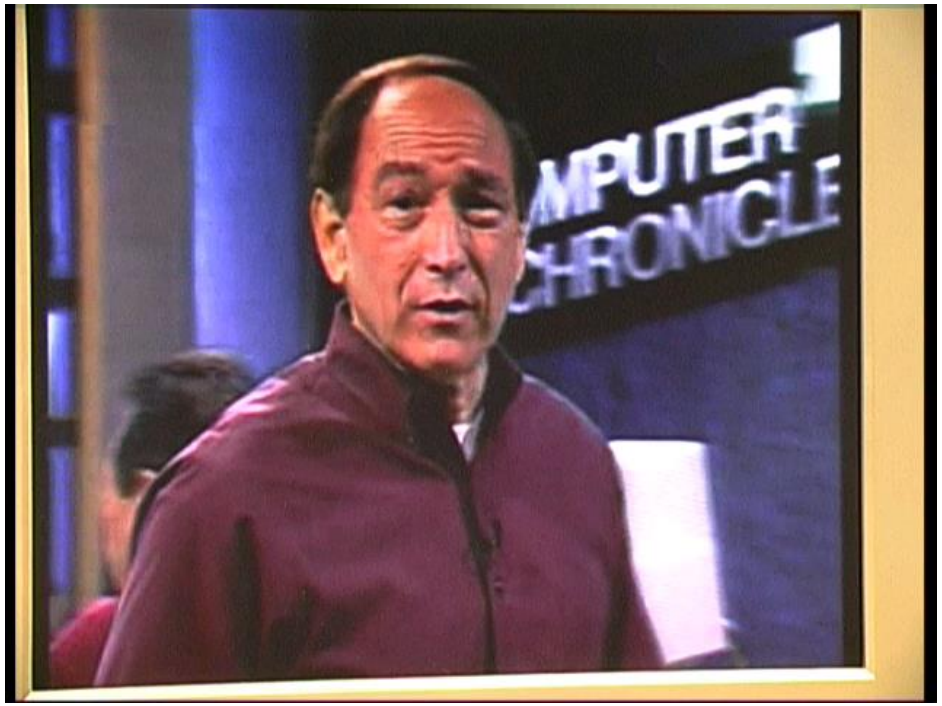
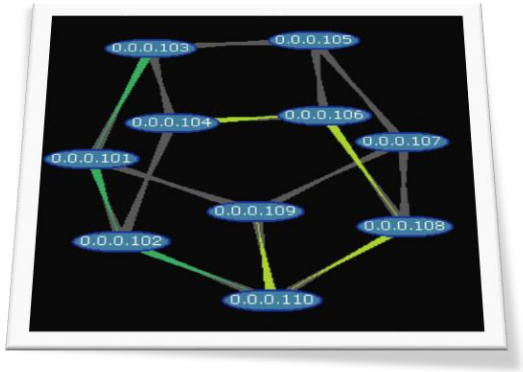
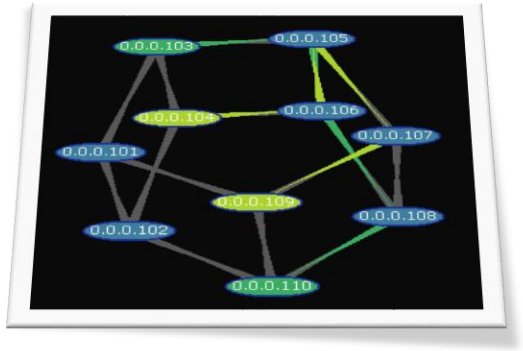


Fig. 4: Comparison of a system without harvesting that uses a battery of size E^o with one that uses energy harvesting. All parameters are as in Figure 1, with $E = B = 100$ for the system with energy harvesting, and we fix $r = 0.1$. The ratio $\log \frac{T_a^o}{T_a}$ is shown in the y-axis, versus the battery capacity of the node without harvesting E^o, for four different values of λ_A. We see that a node that uses a large replaceable battery is potentially more robust. Other parameters are identical to Figure 2.


MPUTER
CHRONICLE





Acknowledgements

Joint Work funded by the European Commission, with BT Exact, FP7 NEMESYS with Telecom Italia, Deutsche Telekom, ATOS, Hispasec, ITI-Certh, UK Technology Strategy Board Project SHIELD, BT-Exact, Northrup-Grumman, Lockheed-Martin, EPSRC ALADDIN with BAE Systems Ltd, MBDA, Finmeccanica,
Cloud Computing Research with SU FP7 ATOS & IBM & LAAS CNRS
Security of Health Systems & the IOT
Current H2020 Projects KONFIDO & GHOST & SerIoT

Imperial College London

CONCLUSIONS

- **Cyber Attacks target Societal Infrastructures, e.g. Health, Transport, Energy, Finance, Education, Manufacturing, Supply Chains, Cities, Safety, Politics, Comfort**
- **There are a Great Variety of Attacks, and More will Come**
- **International Agreements and Regulations are Needed Policing**
- **CyberAttacks are Here to Stay: Everyone is Training More Human Defenders and Attackers (i.e. Cyber Security Experts)**
- **Understanding Cyber Defense goes Hand in Hand with Understanding Cyber Attacks**

CONCLUSIONS

- **The IoT will make things Worse before they Get Better**
- **Research is Needed to Design and Build Resilient Systems**
- **Security and Provenance were not Part of the Initial Design**
- **Could the System be Re-Designed or Substantially Modified?**
- **Who would pay for that?**
- **Is the current Business Model Right? Is there a Role for the EU?**

Thank You for Your Attention

http://san.ee.ic.ac.uk