Adaptive Distributed Mechanism Against Flooding Network Attacks based on Machine Learning

Josep Lluís Berral[1,2], Javier Alonso[1,3], Nicolas Poggi[1], Ricard Gavaldà[2], Manish Parashar[4] and Jordi Torres[1,3]

UPC, Computer Architecture Department[1]
UPC, Software Department[2]
BSC-CNS, Barcelona Supercomputing Center[3]
Rutgers University, Dept. of Electrical and Computer Engineering[4]

AISec'08 [CCS'08] - October 2008

AI and Autonomic Computing

- Applying Machine Learning and AI to Autonomic Computing:
  - Self-* properties and decisions become more accurate.
  - ...so Self-Defence and Self-Protection can be improved and automated.

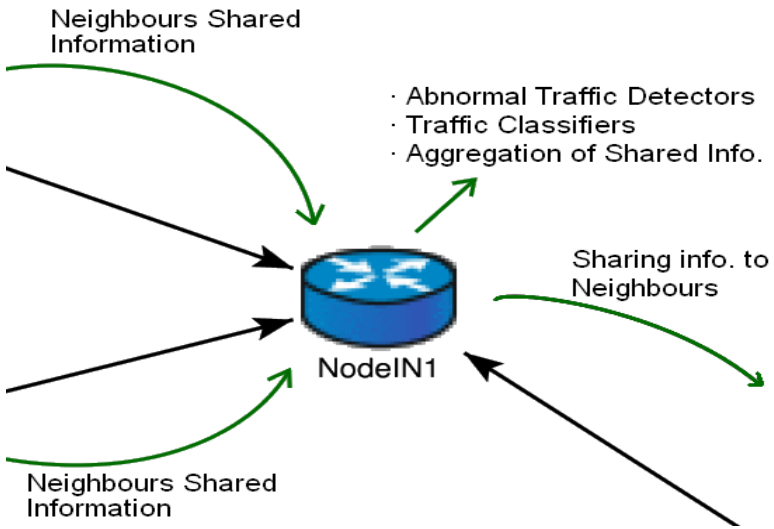
- Challenges for protection against DDoS:
  - DDoS are hard to detect because of the resemblance to legitimate traffic.
  - Single attackers are very difficult to identify.
  - If DDoS follow any pattern, maybe ML can find an accurate classifier.

Introduction

- Using Machine Learning and Data Mining the self-defence properties on a network can be improved.
  - For this case, detect and react in front of DDoS Flooding Attacks.
- Main Contribution:
  - Through information sharing, a network is able to stop and avoid a distributed flooding attack.
  - The system will have the distributed self-protection property, powered by trained classifiers.
  - Self-management implies less human attention on systems. Further, once installed, system self-adapts to any change.

Approach - Architecture

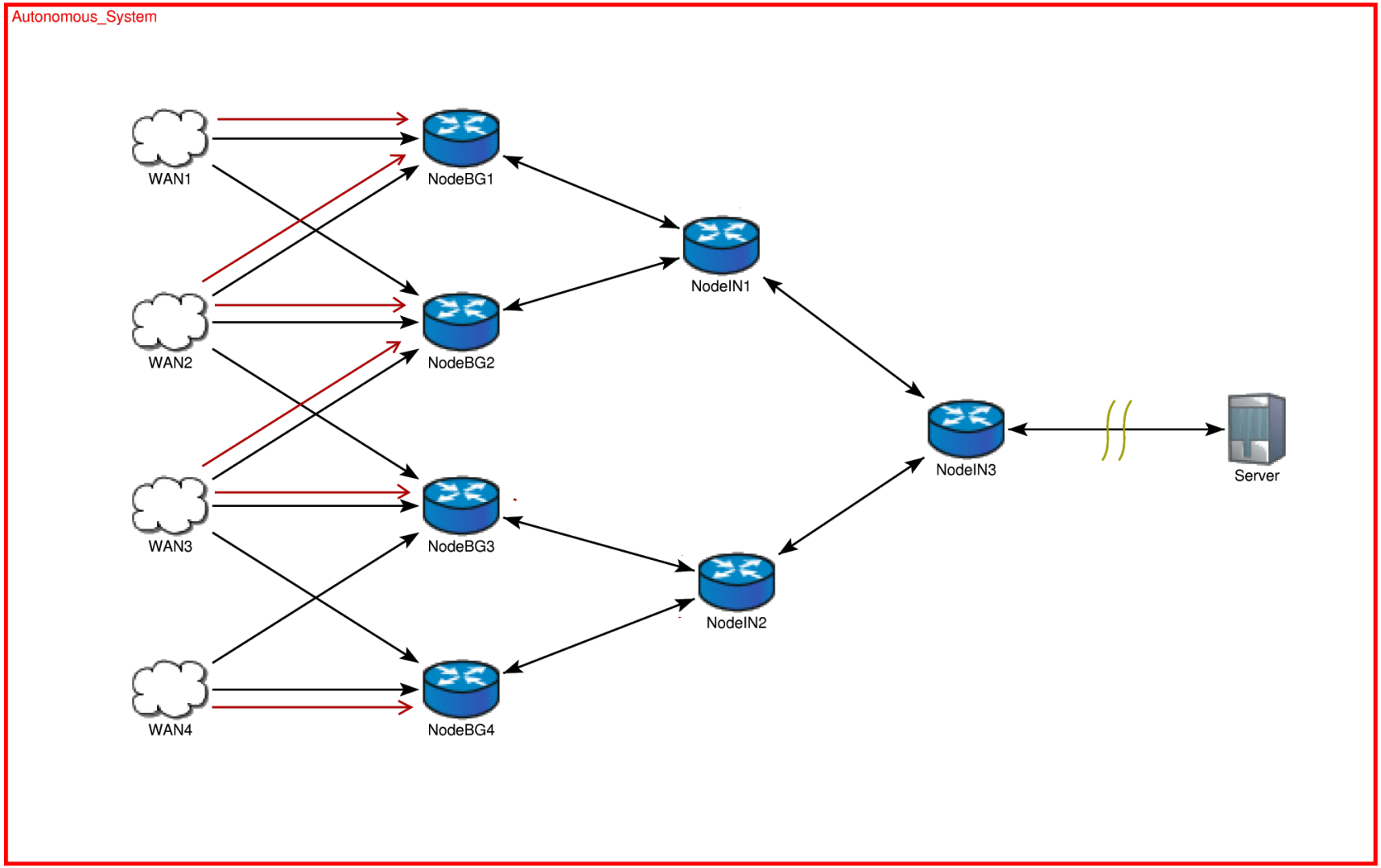
- Overview of the Architecture
  - Nodes in the intermediate network are equipped with detectors, collecting the traffic behaviour.
  - This information is shared with the neighbour nodes.
  - Also, nodes have a trained learner to classify the traffic.
  - Each node uses the aggregated information to improve traffic classification.



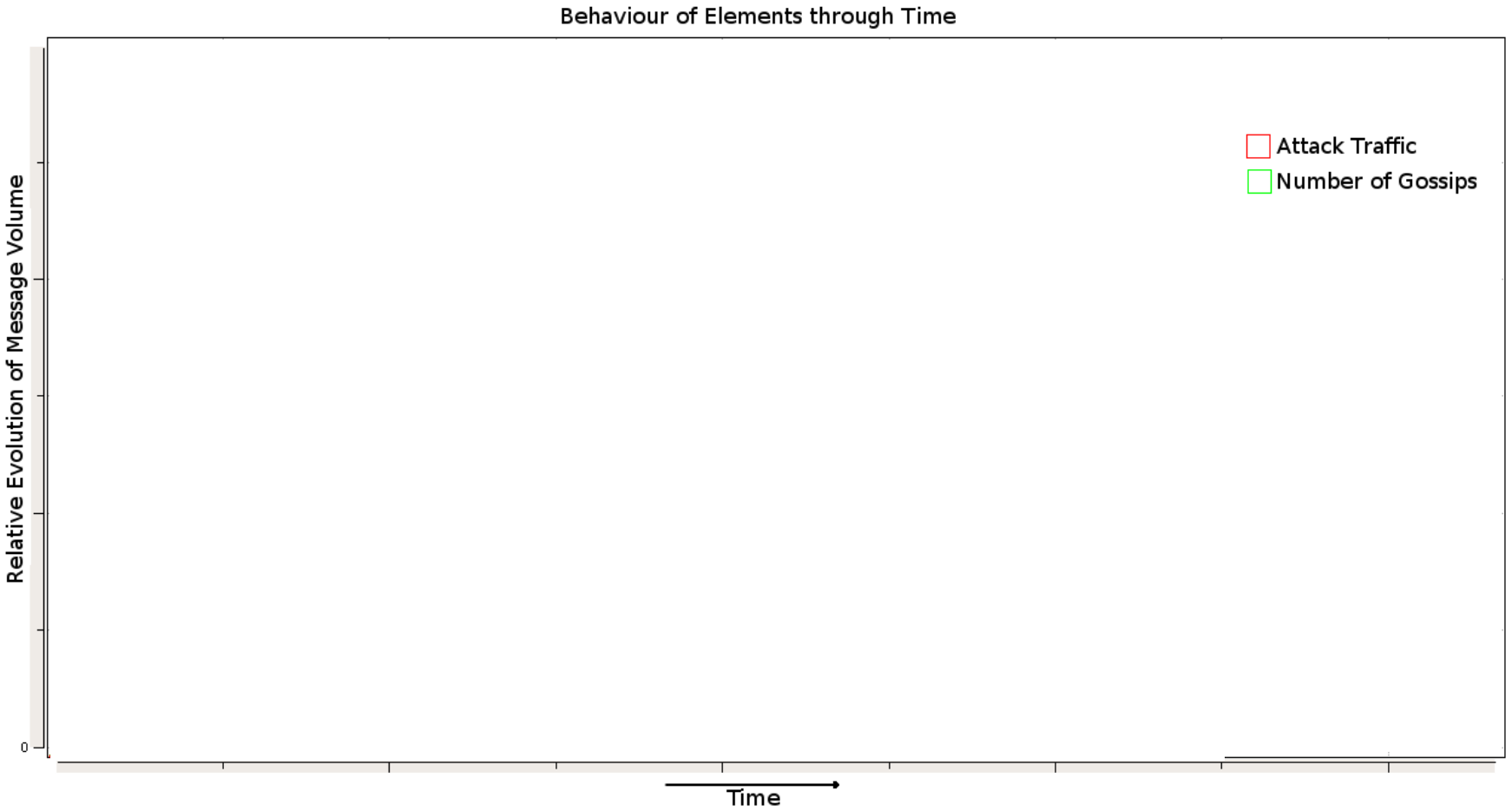
Approach – Architecture (II)

- Detection:
  - Use of “Cumulated Sum” method to detect abnormal increasing of traffic.
- Sharing Information:
  - Gossip confidences about possible victims among neighbours.
  - Warn neighbours about sources classified as attackers.
- Classifying:
  - Naive Bayes method used to classify traffic using source, target, gossips and warnings.

Architecture (III) - Execution



Architecture (IV) - Behaviour



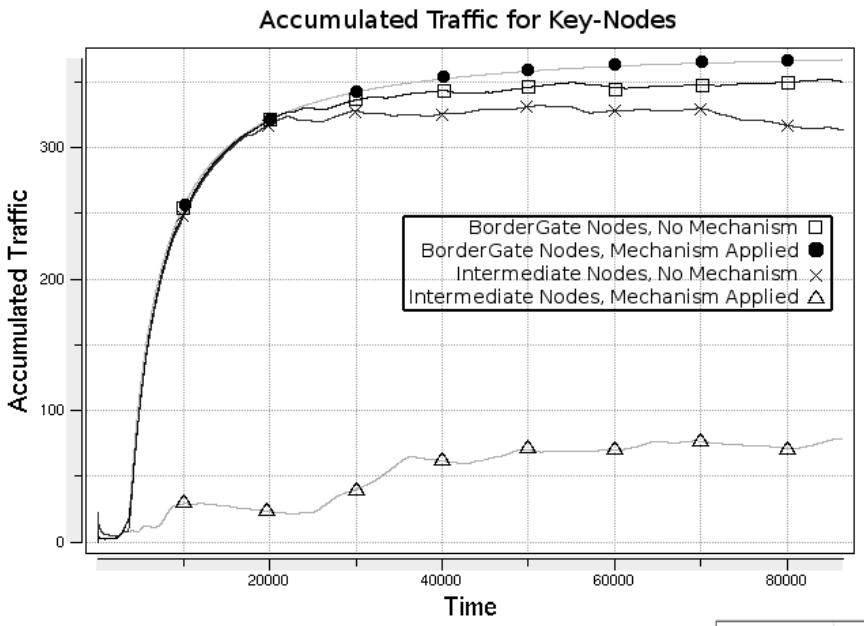
Experimentation

- Theoretical Ad-Hoc Prototype:
  - Prototype implementing traffic and classifiers.
    - View the relevance of the message attributes <protocol, lenght, gossips for the target, warnings for the source, …>
    - System is trained using common clients and attackers.
  - Results:
    - Warnings and gossips have more influence in classification than other attributes.
    - Attack packages are stopped close to the source.
    - The expected behaviour happens in the simulations.

Experimentation (II)

- Network Simulation:
  - Implementation of the mechanism in a simulated network.
    - Observe the behaviour and reaction of the network and the mechanism.
    - Recreation of the main structure of the UPC network.
    - Use of OMNet++ and INET simulation tools.
  - Results:
    - Detectors and Classifiers behave as expected.
    - The detected attack packages are around 95%.
    - When there is no attack, all traffic reaches the target. Also, false negatives are stopped in the intermediate network.

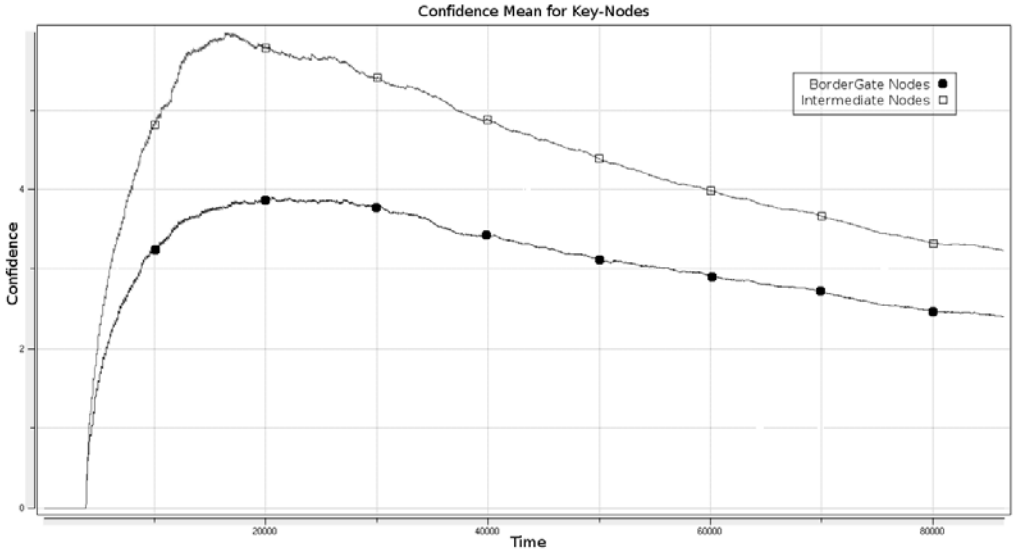
Experimentation (III)



The accumulated Traffic relies on the border gate nodes.

Intermediate nodes rely free of part of the attack.

Gossips maintains the intermediate nodes and the bordergate nodes well informed during the attack.



Conclusions and Future Work

- Challenge and Contribution
  - Improve the Autonomic Computing self-* properties using AI and ML.
  - This work: The DDoS protection mechanisms are tuned and self-adapted using ML and information sharing.
  - The system can take decisions more accurately than using static mechanisms.

- Experimentations
  - Simulating the framework on diverse environments, results are as expected. Confirmation of the expected behaviour of the network.
  - The accuracy of the classifiers is over 95%. Less than 1% of unwanted traffic reaches the victim.

- Future Work
  - Improve on classification and scalability.
  - Teaching the system to recognize other treats, not only DDoS.

Thank you for your attention