Revisiting unstructured overlay network security

Abdelberi Chaabane

Internship at INRIA Planete Team
Supervisor: Mohamed Ali Kaafar

Student talk MITACS 09

Jun 27, 2009

Outline

1. What are Overlay Networks ?
2. Identified Attacks
3. Potential Countermeasures
4. Experiments & Analysis
5. further work

What are Overlay Network ? (I)

- A logical network built on top of a physical network.
    - Increase performance
    - Increase reliability
    - Increase security ?
- Offers new functionalities
    - File sharing
    - Multicast
    - ...
- Easy to deploy !
- E.g.: Skype, ESM ...

Overlay network Type

Structured Overlay network

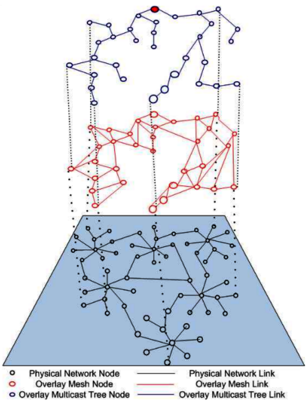
- Neighbor is defined by organizational constraint !
- Bound the number of hops (for searching ...)
- E.g.: Chord, Kademlia ...

Unstructured Overlay network

- No constraint in neighbor selection
- Maximize "some" performance metrics
- E.g.: ESM, Nice ...

Multicast Overlay (I)

- Mimic the Native IP multicast (application Layer).
- Application Layer is responsible of routing mechanism



[1]

[1] Source Walter et al (T.O.N 2008)

Multicast Overlay (II)

Self organization

- No node has a complete view of the network.
- Each node stores
  - Parent
  - Children
  - Peer set (Neighbors)

Tree adaptation

- Metrics collections
  - Passive observation of their own performance
  - Periodic probing of Random peer nodes about their performance
- Compute an utility function
- Decide whether or not changing the parent

Outline

1. What are Overlay Networks ?
2. Identified Attacks
3. Potential Countermeasures
4. Experiments & Analysis
5. further work

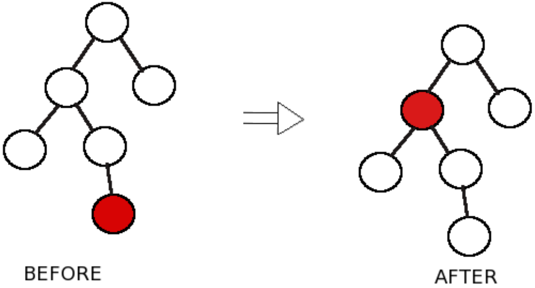
Attacker model

- Byzantine Attack : attacker(s) is a part of the network (insider)
- Attacker has a full access to the data handled by the node
  - Node and Overlay parameters
  - Cryptographic keys
- They can
  - Lie about the observation
  - Impose influence toward the observation (i.e dropping packets)

3 Attacks type

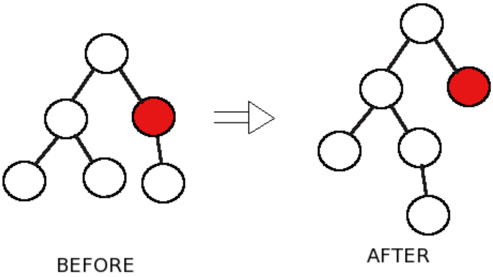
- Attraction attack
- Repulsion Attack
- Disruption Attack

Attraction Attack



- Present the network metrics better than they actually are
- Attract legitimate nodes
- Goal: Perform data analysis, selective data dropping...

Repulsion Attack



- Selfish attack
- reduce attractiveness of the malicious node
- Goal: Have a free-load, and to behave as a free-Rider !

Disruption Attack

- Influence the adaptation mechanism
- Goal: The destruction of the network, D.O.S

Outline

1. What are Overlay Networks ?
2. Identified Attacks
3. Potential Countermeasures
4. Experiments & Analysis
5. further work

Outlier Detection’s Approach

- Walter et al presented [2] a framework for detecting and mitigating these attacks
- based on both spatial & temporal outlier detection

Spatial Outlier

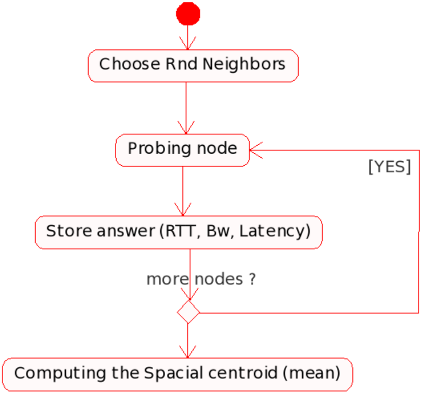
- Compare the reported metrics from each node to the average of all claimed probes (spatial centroid)
- Detect dissimilarities between the node response and "the network" condition

Temporal Outlier

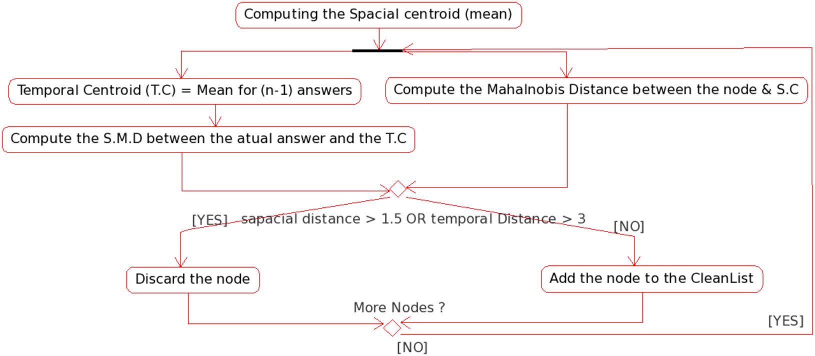
- Compare the reported metrics (n) of the node with its (n-1) previous metrics
- Detect inconsistencies over time by a node

[2] T.O.N 2008

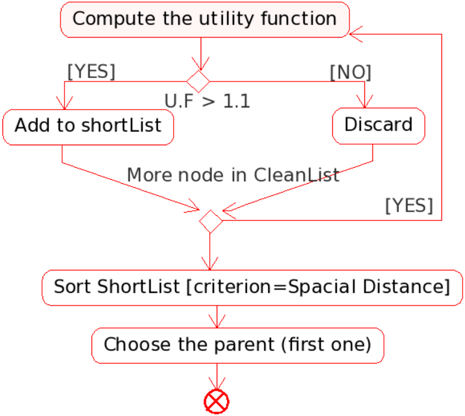
Step1: Collecting Metrics


Choose Rnd Neighbors
Probing node
[YES]
Store answer (RTT, Bw, Latency)
more nodes ?
Computing the Spacial centroid (mean)

Step2: Computing Spatial & Temporal distance


Computing the Spacial centroid (mean)
Temporal Centroid (T.C) = Mean for (n-1) answers
Compute the Mahalnobis Distance between the node & S.C
Compute the S.M.D between the atual answer and the T.C
[YES]
sapacial distance > 1.5 OR temporal Distance > 3
[NO]
Discard the node
Add the node to the CleanList
More Nodes ?
[YES]
[NO]

Step3: Utility function


Compute the utility function
[YES]
[NO]
U.F > 1.1
Add to shortList
Discard
More node in CleanList
[YES]
Sort ShortList [criterion=Spacial Distance]
Choose the parent (first one)

Our goal

- We were interested in overlapping overlay security
- But we found that no approach was suitable for securing even simple overlay
- So we are working on ...

Outline

1 What are Overlay Networks ?

2 Identified Attacks

3 Potential Countermeasures

4 Experiments & Analysis

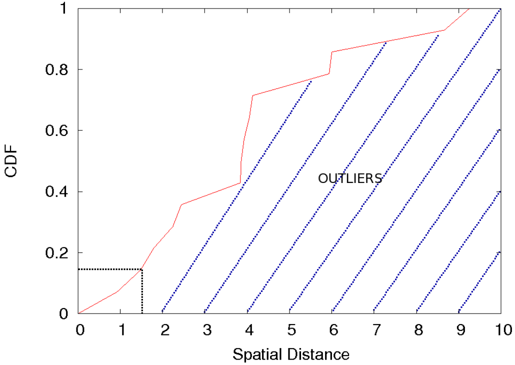
5 further work

Experiments details

- We have implemented ESM
- Real world expermitents on PlanetLab
  - 50 nodes
  - 40 minutes session

Spatial outlier detection

- CDF of the spatial distance in a **no malicious** nodes system
- 80% are outliers based on the proposed threshold
- The test is too aggressive

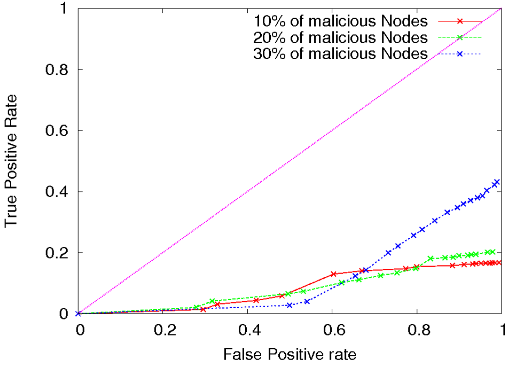


CDF of the Spatial Distance

Temporal outlier detection

- Sensible to sudden changes
- We should not discard automatically the outlier !
- We should define a threshold of the maximum number of succesive reported anomalies

Detection method performance



ROC curves. Each tick on the plots corresponds to a different value of the threshold (significance level, aggressiveness)

Outline

1. What are Overlay Networks ?
2. Identified Attacks
3. Potential Countermeasures
4. Experiments & Analysis
5. further work

What we learned

- Setting a reference set of points, from which we would like to extract outliers is inapplicable
  - Overlay metrics are heterogeneous
  - The "sample" is too small to be Representative of the network conditions
  - Mahalanobis distance is used to measure the dissimilarity between two random vectors of the same distribution

Further works

- Alternatives that are less aggressive
- We have to use a collaborative way of checking
- Reputation-based approach

Questions

Thank you for your attention.

Any questions ?

abdelberi.chaabane@inrialpes.fr

Further infos

- Malahanobis Distance:
  - $d(\vec{x} + \vec{y}) = \sqrt{(\vec{x} - \vec{y})^T C^{-1} (\vec{x} - \vec{y})}$
  - $\vec{x} and \vec{y}$ are vectors which include bandwidth, latency and RTT.
  - $\vec{x}$ is the value from the probe response
  - $\vec{y}$ is the average value thar was calculated (Spatial Centroid)