Automatic Reconfiguration using a Robust Overlay Network and Security Assurance Values

Loïc Baud
Pham Viet Tan Nguyen
Patrick Bellot

with the helpful guidance of Michel Riguidel
Introduction

- This work is the first step towards the LOTM™

- We designed:
  - A robust overlay network named ROSA.
  - A Security Assurance (SA) value computation scheme for system components.
  - A reconfiguration application supported by ROSA and implementing a security policy based on SA values.

- This is a first experience to build and validate the components of the LOTM.

The Demo Application

Reconfiguration application

Data $\rightarrow$ SA Values $\rightarrow$ Decision

Sensors  Topology

Reconfiguration command
Description of ROSA
The Overlay Network

Loïc Baud, PhD Student
ROSA (Introduction)

- ROSA stands for: **Robust Overlay with Self-Adaptive topology**
- ROSA is a scalable overlay network. No limits.
- ROSA provides a failure-tolerant routing.
- ROSA takes into account the evolution of the underlying IP topology (failures and recoveries) to reconfigure itself.
- ROSA is implemented in Java, very soon in C++.
- ROSA is deployed on the INFRES network.
ROSA (Description)

- ROSA can be seen as a set of intermixed RON called lumps.
- A **lump** is a set of virtually fully interconnected nodes.
ROSA (Lumps)

- The nodes are permanently trying to modify lumps to increase the connectivity.
- The core of ROSA is the reconfiguration algorithm:
  - To permanently increase the connectivity.
  - To take into account the underlay network failures.
ROSA (Density of a Lump)

- The **density** of a lump \( l \), noted \( \delta(l) \), is the minimum number of underlay link failures that are sufficient to isolate a node of the lump.

- Underlay network

- Overlay network

- Densities

\[ d = 2 \]

\[ d = 1 \]
In a valid configuration, there exists a path of lumps between any pair (a,b) of nodes.

The density of a path s between a and b, noted $\delta_p(s)$, is the minimum of the densities of the lumps composing the path.

It is the minimum number of underlay link failures sufficient to break the path.
ROSA (Connectivity between a Pair of Nodes)

- The connectivity between a pair of nodes \((a,b)\) is defined as the maximum of the densities of the non-cyclic paths between \(a\) and \(b\).
- It is noted \(\delta_c(a,b)\). It is sure that if less than \(\delta_c(a,b)\) underlay links fail, then the connection between \(a\) and \(b\) remains. It is not the best possible index.
The goal of reconfiguration is to improve the connectivity index of the network.

The reconfiguration is done on a step-by-step basis using only local node information.

A successful reconfiguration step is a step strictly increasing the connectivity index of the network.

Of course, reconfiguration is concerned only with valid configurations.
Security Assurance Values
Computation

Nguyen Pham, PhD Student
SA Values

- The SA Value of a system component reflects the objective confidence we have in the normal behavior of the component from the point of view of availability and security.

- SA Values are computed with two visions:
  - The static vision is a reflect of the components configuration and system topology.
  - The dynamic vision takes into account the running states of the components.
SA Values

- SA Values are computed for:
  - Workstations.
  - Servers.
  - Routers.
  - Subnetworks (Ethernet).
  - The whole system.

- SA Values are computed from measures coming either from SNMP queries or from scripts.
According to the static configuration of a system, an attack graph is statically built.

- E.g. if login is successful on a machine, rlogin may allow to reach all other machines.
- E.g. if FTP is successful on a machine, NFS allows this FTP to get all files of the mounted disks.

Attackability: the likelihood of a successful attack is computed from the attack graphs and normalized in $[0,1]$. It is a static value.
Workstation and Server SA Values

- For each station/server we compute the local processing capability and the local networking capability.
- The processing capability is the min of seven normalized values.
- The networking capability is the min of six normalized values.
- Finally, the dynamic SA Value is the min of the two capabilities.
Workstation and Server SA Values

- Example: computing networking capability
  - IPR: Input Packet Rate (10 sec.)
  - IPER: Input Packet Error Rate (10 sec.)
  - OPR: Output Packet Rate (10 sec.)
  - OPER: Output Packet Error Rate (10 sec.)
  - PCR: Packet Collision Rate (10 sec.)
  - OUP: Open UDP Ports (30 sec.)
  - ODD: Output Datagram Discarded Rate (30 sec)
  - IDD: Input Datagram Discarded Rate (30 sec)
● Example continued: computing networking capability

- The 5 first values form a group (IPR, IPER, OPR, OPER, PCR) giving a value reflecting the good health of networking:

  \[ 1 - \frac{(IPER + OPER + PCR)}{(IPR + OPR)} / 0.05 \]

- The second computed value is: IPER / IPR
- The third computed value: OPER / OPR
- The fourth computed value is: OUP / Threshold
- The fifth computed value is: ODD / Threshold
- The sixth computed value is: IDD / Threshold

● The computing capability is the min of these six values.
Workstation and Server SA Values

- The final SA Value of a workstation and a server is the minimum of:
  - The static SA Value (attackability)
  - The networking capability (dynamic SA Value)
  - The processing capability (dynamic SA Value)

- The difference between the workstations and the servers lies in the different thresholds.
Router SA Values

- Routers SA Values are computed in the same way as workstations and servers SA Values except that there is no static SA Value and that measured values are not exactly the same.

- Routers SA Values are computed by distant workstations using remote SNMP measurements.

- This workstation has to be randomly chosen at each turn to avoid single point of failure.
Subnetwork SA Values

- The subnetwork SA Value is computed as the minimum of:
  - The average of the SA Values of the workstations composing the subnetwork.
  - The average of the SA Values of the gateways of the subnetwork.
  - The networking capability of the subnetwork computed in a similar way to the networking capability of a workstation.
- The SA Value is computed by a randomly chosen workstation.
System SA Values

- Each subnetwork has a weighted SA Value.
- The weight is proportional to the number of machines of the subnetwork.
- The system SA Value is the weighted sum of the subnetworks SA Values.
Future Works

- Simulation for large system.
- Propagation of SA Values (Distributed Computation Model).
- Metrics taxonomy.
The Demo Application

Patrick Bellot
The Demo Application

- ROSA helps computing SA Values.
- ROSA collects SA Values.
- The Application reconfigures the underlying IP.
- All application communications are handled by ROSA.
- An applet shows the current state (for demo only).

- Note: IP reconfiguration is virtual because we do not want to really modify the INFRES Network.
The Demo Application
Security Policy

- We implemented a very simple security policy:
  - When a router or a gateway has its SA Value decreasing below a threshold value, then we reconfigure IP routing to use another path.
  - When an Ethernet subnetwork has its SA Value decreasing below a threshold value, e.g. infected by a virus, we reconfigure IP to isolate this sub network.
Future Works

- To keep the ROSA concept but forget about overlay ideology.
- Makes ROSA reconfigure itself according to SA Values.
- To add applicative functionalities to ROSA:
  - Distributed communications for commands & events.
  - Distributed storage for surveillance data.
  - Distributed computation to compute surveillance data.
- To improve SA Values computation using new paradigms.
- ROSA is a candidate to LOTM award.