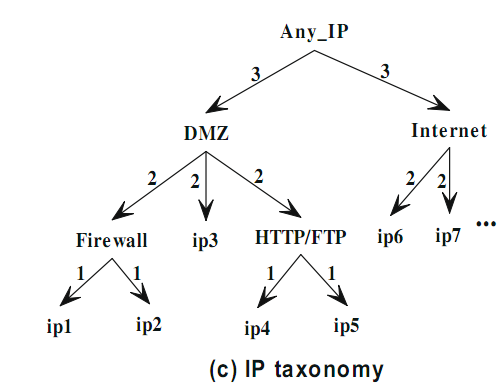
# Intrusion detection alarms reduction using root cause analysis and clustering

Paper này cải tiến cái paper của Julisch ở 1 số điểm

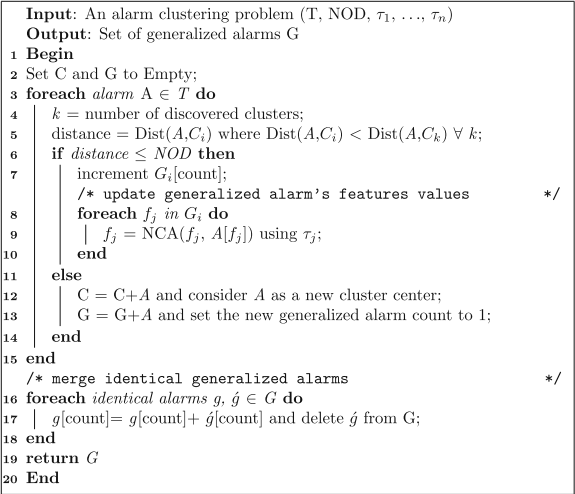
* Đánh trọng số cho các cạnh của generalization hierarchies



* Dùng nearest common acncestor(NCA) thay vì parent trực tiếp
  + Lúc này ip5 gần ip1 hơn Internet thay vì kiểu cũ thì 2 giá trị này như nhau
* Sử dụng khoảng cách giữa các cluster (trong paper gọi là NOD): khoảng cách giữa các cluster phải <= NOD.

Giải thuật

* Ý tưởng của giải thuật: tìm clusters mà khoảng cách giữa các alert <= NOD sau đó tạo 1 generalized alert cho mỗi cluster
* Các bước:
  + 1 tập các alert chứa nhiều cluster
  + Mỗi cluster có chứa nhiều alert và khoảng cách giữa các alert <= NOD
  + Tạo generalized alert cho mỗi cluster bằng cách tìm NCA cho từng thuộc tính.(line 6-13)
  + Gộp các generalized alert giống nhau lại (line 16-17).
  + Trả về kết quả
* Mã giả



* 1 số nhận xét
  + Line 5: tìm cluster gần nhất để gắn alarm A vào
  + Line 8-9: cập nhật giá trị của generalized alert của cluster i bằng cách tìm NCA của alert A và generalized alert Gi
  + Giải thuật này cũng có thể áp dụng chạy realtime vì khi thêm alert mới vào nó cũng thực hiện so trùng với generalized alert.
* Sau khi tìm được các generalized alert sẽ dùng chúng để filter các alert mới.

Chọn giá trị của NOD, có 2 cách có thể kết hợp cả 2 cách:

* Giá trị của NOD tùy thuộc vào generalization hierarchies của thuộc tính đó
  + Cao nhất bằng longest path của cây đó
  + Thấp nhất bằng shortest path của cây đó
* Giá trị của NOD đc xác định bằng cách chạy giải thuật nhiều lần và xác định giá trị tốt nhất bằng cách đánh giá cluster.