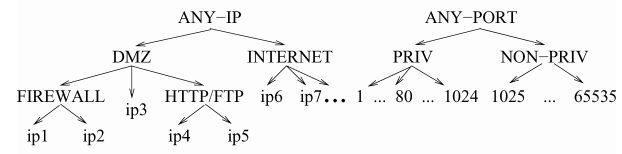
# Clustering Intrusion Detection Alarms to Support Root Cause Analysis

1. Định nghĩa
   * Assumption:
     1. Các alarm cùng 1 root cause thường similar
     2. Mỗi cluster đều có thể biểu diễn bằng 1 generalized alarm
   * Root cause của 1 alarm là nguyên nhân mà alarm này đc raise
   * Root cause analysis: xác định root cause và các thành phần mà nó ảnh hưởng
   * Alarm: là 1 tuple trên miền tích Đề các của các attribute dom(A1)xdom(A2)…xdom(An) với A1..n là thuộc tính của alarm
     1. Các thuộc tính này ko giống IDMEF vì IDMEF có dạng phân cấp
   * Alarm log là tập hợp các alarm
   * Giá trị tổng quát của 1 thuộc tính (generalized attr value) là 1 tên chỉ 1 tập con của dom(Ai)
     1. Ví dụ: weekdays là generalized attr value của thứ 2,3,4,5,6
   * Extended domain – Dom(Ai): của 1 thuộc tính là hợp của dom(Ai) và generalized attr value của dom(Ai)
     1. Ví dụ: thứ 2 ,3,4,5,6,7,weekdays
   * Generalized alarm là 1 tuple của hiệu của tích các extended domain và tích của các domain.
   * Generalization hierarchies: mỗi attribute đều có 1 graph Gi là generalization hierarchies. Thật ra nó có thể là 1 DAG hay tree. Node cha là tổng quát của các node con của nó.



* + 1. 1 alarm a đc gọi là cha của 1 alarm b khi tất cả các thuộc tính của a đều là cha của tất cả thuộc tính của b
       1. Ví dụ: alarm có 2 thuộc tính {thứ 2, 192.168.1.1} sẽ là con của alarm {weekdays, 192.168.1.1}

1. Bài toán
   * Exact alarm clustering: cho 1 alarm log, nhóm tất cả các alarm vào các cluster sao cho các alarm trong cùng 1 cluster có cùng 1 root cause
     1. Nói chung ko thể có 1 giải thuật nào có thể giải bài toán này vì cái này chỉ là mô hình lý thuyết
   * Approximate alarm-clustering :
     1. Assumption: root cause của 1 alarm cluster có cấu trúc nhất định (structural properties)
     2. Approximate alarm clustering sẽ tìm những alarm cluster có những cấu trúc này thay cho việc giải exact alarm clustering.
        1. Hay cho 1 alarm log, bài toán này sẽ tìm những alarm cluster lớn mà **có thể** biểu diễn được bằng generalized alarm
           1. Bài toán này dựa trên 1 tiền đề: root cause thường tạo ra rất nhiều alarm mà các alarm này **có thể** biểu diễn bằng generalized alarm
           2. Ngoài ra phải định nghĩa có thể biểu diễn nghĩa là ntn và 1 alarm cluster như thế nào là lớn
     3. Định nghĩa khác: L là 1 alarm log, min\_size là 1 integer, Gi là 1 generalization hierarchies của 1 thuộc tính Ai. Bài toán đc xác định như sau: tìm 1 tập C là con của L mà cực tiểu hóa H©và thõa ràng buộc số phần tử trong C >= min\_size
        1. Min\_size là 1 khái niệm dùng để xác định 1 cluster như thê nào là lớn
     4. Bài toán này là bài toán NP-complete: chứng mình dựa vào việc chuyển bài toán CLIQUE về bài toán này. CLIQUE là gì cũng ko quan trọng => phải tìm heuristic
   * Một số sample root causes và generalized alarm của nó
     1. A HTTP server with a broken TCP/IP stack that fragments outgoing trafﬁc.

“Fragmented IP” alarms ensuewhen the server responds to clients requests.

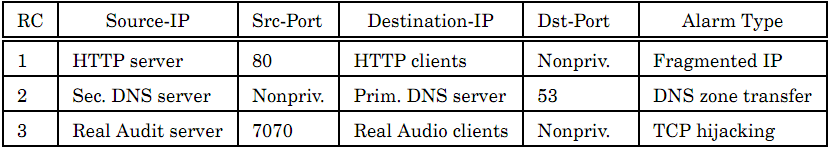
* + 1. At one site, a misconﬁgured secondary DNS server performed half-hourly

DNS zone transfers fromthe primary DNS server. The resulting “DNS zone

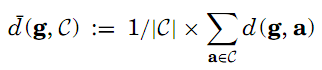
transfer” alarms are no surprise.

* + 1. A real audio server whose trafﬁc remotely resembles TCP hijacking at-

tacks. This caused our commercial IDS to trigger countless “TCP hijacking” alarms



* + Định nghĩa có thể: 😐
    1. Khái niệm dissimilarity d(.,.):
       1. Nhận 2 alarm vào và trả về 1 số chỉ độ khác nhau của 2 alarm đó. Độ khác nhau này xác định khả năng (có thể) của 2 alarm có thể tạo thành 1 generalized alarm
       2. Việc xác định dissimilarity dựa vào generalization hierarchies và do người dùng xác định
    2. Dissimilarity giữa 2 attr
       1. Bằng shortest path giữa 2 node này trên generalization hierarchies thông qua 1 node cha chung là p
          1. Ví dụ: d(ip1,ip1)=0, d(ip1,ip4)=4, d(PRIV,NON-PRIV)=2
    3. Dissimilarity giữa 2 alarm
       1. Bằng tổng của dissimilarity của các thuộc tính của nó
          1. Việc này xem các thuộc tính là như nhau ko có cái nào quan trọng hơn cái nào => có thể phát triển ý tưởng này
    4. Khái niệm heterogeneity H(C) của 1 alarm cluster C (heterogeneity: tính ko đồng nhất)
       1. Heterogeneity là 1 hàm trả về 1 giá trị càng nhỏ khi cluster C có thể biểu diễn bằng generalized alarm
       2. Công thức tính heterogeneity: giả sử g là 1 generalized alarm của 1 cluster C (tức g là cha của tất cả các alarm của cluster C)
          1. Average dissimilarity d(g,C) giữa g và C đc tính như sau:



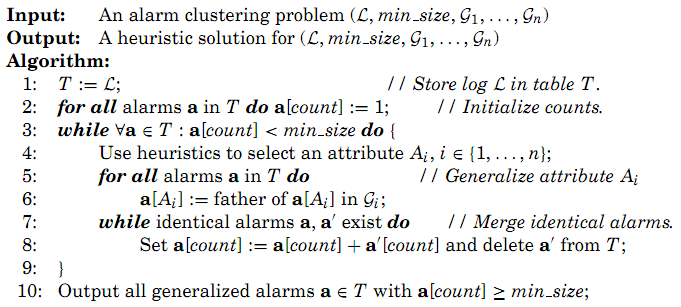
Trung bình cộng của khoảng cách từ mỗi alert tới generalized của nó

* + - * 1. Heterogeneity đc tính như sau:



* + 1. Khái niệm cover: 1 generalized alarm g mà với các con của n1o đều thuộc cluster c và có average dissimilarity của g và C = H© gọi là cover của C
       1. Cover của C có thể mô hình cho cluster tốt nhất

1. Giải thuật heuristic để giải:
   * Giải thuật heuristic sẽ tìm cluster có size > min\_size nhưng có thể ko thỏa việc minimize H©
     1. Đây là 1 dạng của attribute oriented induction (AOI)???
     2. Tác giả sử dụng giải thuật tương tự AOI nhưng sẽ có điều kiện dừng khác. **Điều kiện dừng sẽ tương tự density-based clustering**
     3. Ý tưởng chính: cho 1 alarm log L, giải thuật sẽ input là L và generalize L
        1. Generalize đc thực hiện bằng cách chọn 1 attr Ai
        2. Thay Ai của tất cả các alarm trong L bằng parent của nó trong Gi
        3. Kết thúc khi tìm đc 1 alarm cluster với min\_size. Return cái này về.
   * Hiện thực:



* + Dòng số 4: heuristic mà tác giả chọn:
    1. Gọi Fi= max{fi(v)|v thuộc Dom(Ai)} là cực đại của hàm fi(v)= SELECT sum(count) FROM T WHERE Ai=v
    2. Có thể change cái heuristics này cũng là 1 ý tưởng