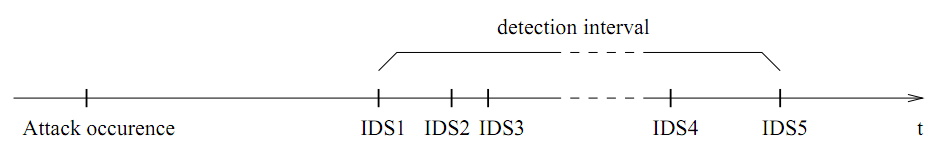
# Using an Intrusion Detection Alert Similarity Operator to Aggregate and Fuse Alerts

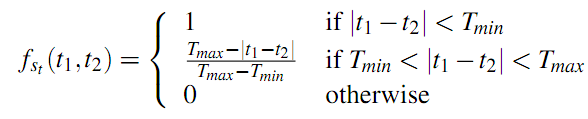
1. Introduction
   * Tại sao phải dùng nhiều IDS kết hợp?
     + Dùng 1 sẽ giảm số lượng tấn công có thể phát hiện đc
     + Dùng nhiều tăng số lượng cảnh báo
   * Tại sao phải kết hợp alert?
     + Lượng alert là rất lớn không phù hợp với human
     + Lượng alert nhiều nhưng thông tin thì ít
   * Kết hợp alert
     + Similarity scale từ [0;1]
2. Các công việc liên quan
   * Probabilistic Approach
   * [Julisch]
     + 1 dạng clustering
     + Cho rằng alert root cause là do config sai
   * Debar Wespi
     + Duplicate definition: 1 alert phải đc thấy nếu 1 alert trc đ1o xuất hiện
3. Độ tương tự của các Alert
   * Mô hình alert
     + Có nhiều cách mô hình alert
       - Dùng feature(ko rõ) [VS01]
       - Dùng 1 tập các attr (kiểu IDMEF)
         * Dùng IDMEF vì khả năng sử dụng với nhiều IDS
     + 1 tập E các event type ???
       - Có thể tạo các alert
       - 1 alert là 1 instance của 1 element của E
       - Associate an event and a set of properties linked to this event to an alert
   * So sánh các thuộc tính
     + Có 4 loại thuộc tính
       - Catergorical: IP,port
       - Numerical:counter, packet size
       - Temporal: numerical nhưng có tính tuần hoàn
       - Chuỗi string
     + So sánh thời gian
       - 1 alert có thể đc detect bởi nhiều IDS. Mỗi IDS có khả năng xử lí khác nhau nên detect time cũng khác nhau.



* + - * + Sớm nhất
        + Lâu nhất

Cái này là train ???

* + - * Xét 2 trường hợp để xác định 2 temporal window cho từng traffic
        + Ko traffic => Tmin
        + Neutral trafiic => Tmax
      * Công thức



* + - * + Chỉ áp dụng đc nếu các IDS đc đồng bộ
    - So sánh IP Address
      * Dựa vào topology của mạng: đọc [Jul03] để rõ
        + Nếu 2 IP cũng subnet thì similarity cao hơn
        + Dựa vào cây IP (IP address taxonomy)
      * Cách tính
        + Dựa vào khoảng cách của 2 IP trong taxonomy tree
        + Similarity value= inverse of the maximal distance minus the calculated distance ???
    - So sánh dữ liệu của User (User data)