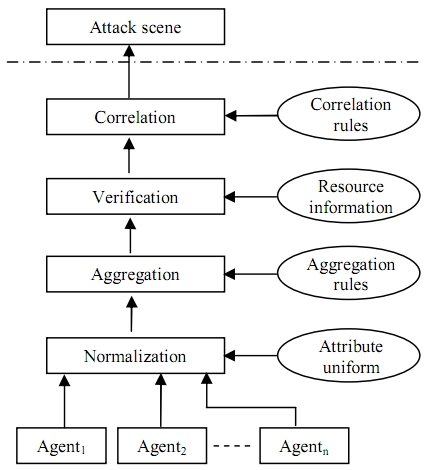
# A survey of Alert Fusion Techniques for Security Incident

1. Introduction
   * Cũng như các paper khác tác giả nêu lên các lí do tại sao phải fuse alert lại
   * Các step thực hiện như trong hình
   * 
2. Alert normalization
   * Dùng IDMEF
   * Tác giả đề xuất việc sử dụng NTP (Network Time Protocol) để synchronize giữa các sensor
3. Alert aggregation
   * Mục đích: gọp các alert có thời gian gần nhau và có tính chất giống nhau(dựa trên attr)
   * Similarity-based[4]-[8]: bằng cách đo khoảng cách giữa các alert
   * Implicit aggregation[9]: 1 alert được xem xét trong không gian 3 chiều (src,dest,class). Các alert sẽ được gọp lại với nhau dựa trên phép chiếu ???
   * Julrisch[10]: paper này đã report
4. Alert Verification
   * Mục đích: lấy 1 alert, xác định xem attack đó có thành công hay không. Mục tiêu là những false alert sẽ bị loại và ảnh hưởng của nó tới quá trình correlate là thấp
   * Có 2 phương pháp:
     1. Passive: cần 1 số thông tin trc về host, topology ...
        1. Ưu điểm là không ảnh hưởng tới network, không cần phải chạy thêm test
        2. Nhược điểm: database cần phải cập nhật
        3. Tiêu biểu của phương pháp passive là M-Correlator (đã report)
     2. Active: kiểm tra xem attack đã thành công không bằng cách check
        1. Nhược điểm: ảnh hưởng tới network, cần phải loại bỏ những alert sinh ra bởi việc test khỏi quá trình correlate ...
        2. Có thể log in vào hệ thống để kiểm tra
        3. Tác giả đề xuất việc sử dụng HIDS để kiểm tra => đây có thể là 1 lí do phải dùng HIDS nữa.
5. Correlation
   * Mục tiêu: xác định mối quan hệ giữa các meta-alert sinh ra bởi aggregation. Có 3 phương pháp chính
     1. Correlation of attack scene:
        1. [12]-[18]: sử dụng các rule hay các scenario template đã có sẵn để nhận diện alert
        2. [19],[20] sử dụng các attack language. Như paper [20] sử dụng chronicle (cái này đọc rồi thấy không áp dụng được!) Vấn đề đối với phương pháp này là làm thế nào để tìm được các pattern.
        3. [21] xây dựng State Transition Analysis Technique (STAT) để mô hình và phát hiện các incident.
        4. [22] xây dựng ngôn ngữ CAML (cái này Thi đọc rồi)
        5. [23] xây dựng 1 phương pháp correlate phi tập trung (decentralized). Tác giả xây dựng 1 giải thuật peer-2-peer để phát hiện các pattern định sẵn. Pattern này được định nghĩa bằng 1 ngôn ngữ.

=>tác giả cho rằng các phương pháp trên đều có thể xác định mối quan hệ giữa các alert nhưng cần phải có pattern sẵn(nhược điểm)

* + - 1. [31] sử dụng Fuzzy Cognitive Maps ( kết hợp của fuzzy logic và neural network). [31] sử dụng cognitive model và FCM đã được dựng sẵn bởi expert để phát hiện tấn công. Theo như paper thì các pattern được xây dựng ở mức abstract nên có thể correlate ngay cả nếu thiếu alert. Tác giả cho rằng pp này có 2 ưu điểm (không thấy nhược) là thiếu alert vẫn correlate được và việc link 2 alert dựa vào evidence của cả 2 alerts.
    1. Pre-post
       1. [23]-[27]: sử dụng pre-post
       2. [28]-[29]: sử dụng predicate để biểu diễn pre-post(của anh Peng Ning). Tác giả cho rằng tool của anh Ning chỉ xài được offline đối với các database có sẵn :| Ưu điểm là có thể loại bỏ false alert tốt :D
       3. [30] tác giả đề xuất sử dụng Hidden Colored Petri-Nets để mô hình hóa. Không rõ về cái này nhưng nó có cả quá trình training. Nhược điểm là cần phải mô hình hóa các attack nên nếu có attack mới thì không thể kết hợp với các attack cũ (có thể do nó train dữ quá nên bị overfit)
    2. Statistical analysis (anomaly detection)
       1. [32][33] sử dụng Granger Causaliti Test (đã từng đọc cái này nhưng rất khó hiểu :| ) Nói chung, nó sử dung time series analysis. Group các alert trong small time window dựa trên các thuộc tính giống nhau.
       2. [34]: tiếp tục sử dụng GCT nhưng có cải tiến về các parameter

1. Kết luận:
   * Tác giả đề xuất nghiên cứu intention recognition để có reaction. Cái paper này năm 2008 nên nếu chọn reaction hay intention thì có thể chưa ai ngâm cứu.
2. Note:
   * Mấy cái paper này không thấy paper nào nói về kết hợp với HIDS => có thể 1 hướng đi