Detección de anomalías en entornos de red aplicado a la identificación de tráfico hostil

19 OCTUBRE 2007

Índice

- Introducción
- Anomaly Detection in IP Networks
- Mining Anomalies Using Traffic Feature Distributions
- Otros trabajos
- Conclusiones

Introducción

- Técnicas para la detección de intrusiones:
  - Misuse detection
  - Anomaly detection
    - Basado en reglas
    - Máquina finita de estados
    - Patrones
    - Análisis estadístico
      - ANOMALY DETECTION IN IP NETWORKS
      - MINING ANOMALIES USING TRAFFIC FEATURE DISTRIBUTIONS

Anomaly Detection In IP Networks

Introducción

- Tesis: *Las anomalías de red están caracterizadas por cambios transitorios correlados en los datos de red medidos antes o durante el evento.*
- Procesado de señales
- Detección de cambios abruptos correlados en los datos
- Centrado en el Router
- Variables SNMP MIB.

Anomaly Detection In IP Networks

Datos

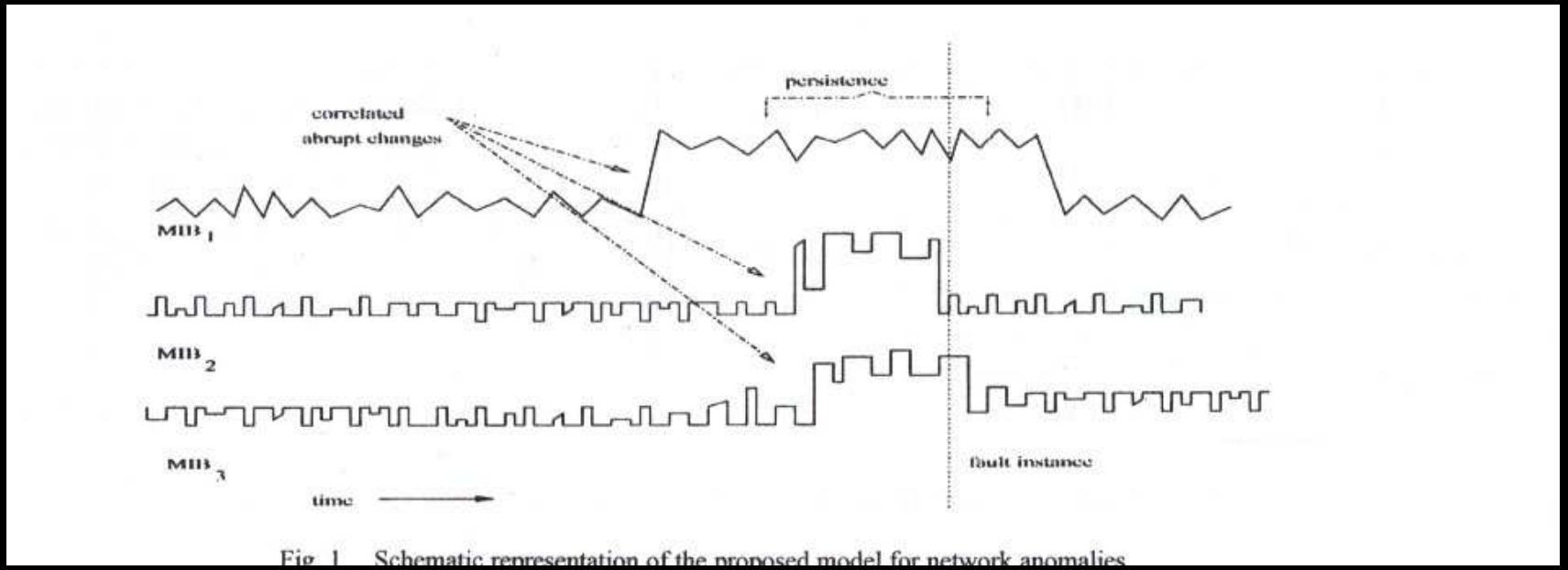


Fig. 1. Schematic representation of the proposed model for network anomalies.

- Se centra en las variables:
  - IpIR
  - IpIDE
  - IpOR
- Correlación cruzada entre las variables
- Ventana de 5 minutos

Anomaly Detection In IP Networks

Procedimiento

- Detectar cambios en las estadísticas de variables individuales
  - 2 Ventanas: Entrenamiento y testeo
  - Varianza de los datos residuales (obtenidos por AR)
  - Cambios -> Test Máxima Verosimilitud (GLR)
- Se obtiene un indicador de anormalidad por cada variable

Anomaly Detection In IP Networks

Procedimiento

- Obtención de la función de salud:
  - Se utiliza un operador lineal
    - Basado en la correlación entre las variables
- Para activar las alarmas se utilizarán Lags con los fallos esperados.
- Anomalías sin Lag serán falsas alarmas
- Casos estudiados:
  - Fallo en el servidor de ficheros
  - Problemas de acceso a la red
  - Implementaciones de error en los protocolos

Índice

- Introducción
- Anomaly Detection in IP Networks
- Mining Anomalies Using Traffic Feature Distributions
- Otros trabajos
- Conclusiones

Mining Anomalies using Traffic Features Distributions

Introducción

- Observación: Las anomalías inducen cambios en las distribuciones de las cabeceras de los paquetes

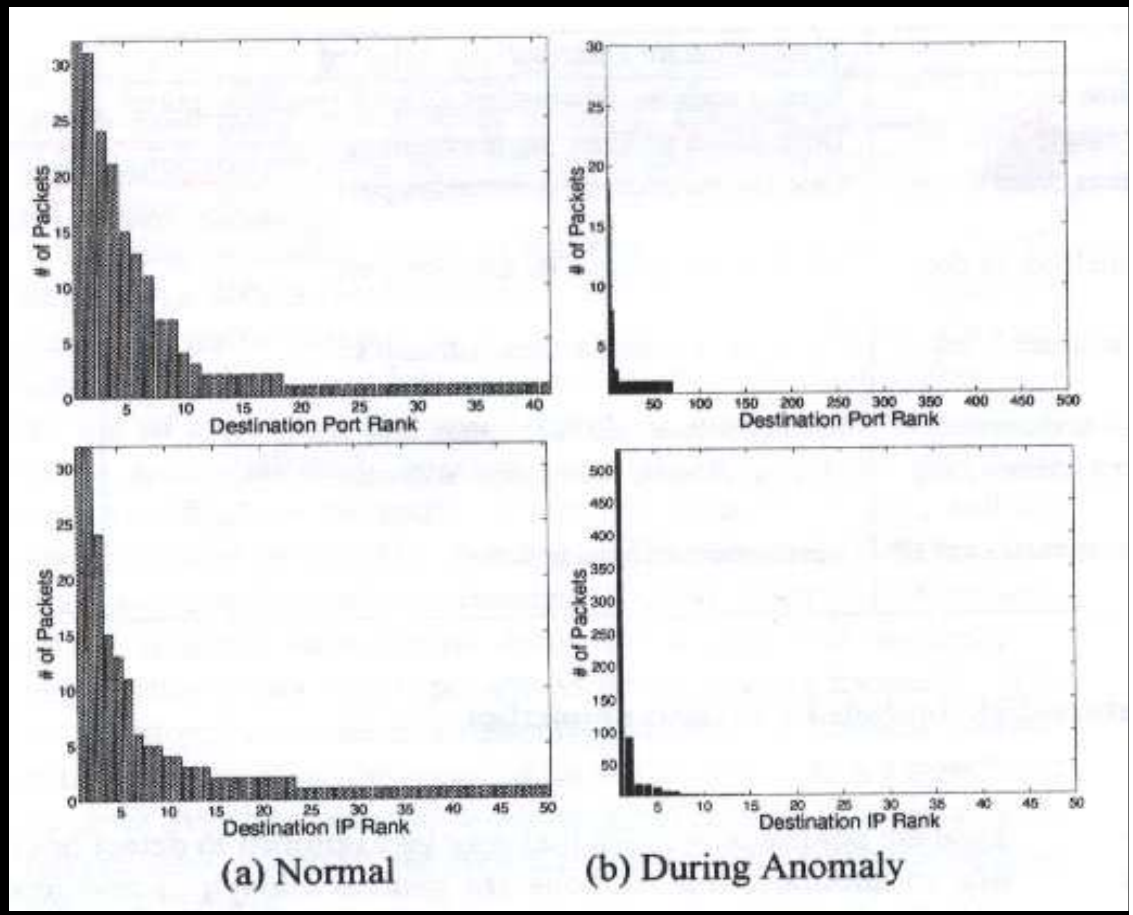
Ejemplo Anomalías		
Nombre Anomalía	Descripción	Distribuciones Afectadas
Flujos alfa	Grandes volúmenes de flujo punto a punto	Direcciones origen y destino (Posib puertos)
DOS	Denegación de servicios	Direcciones origen y destino
Flash Crowd	Inusuales picos de tráfico a una sola dirección, de un origen típico	Dirección destino y puerto destino
Escaneo de puertos	Probar diferentes puertos destino de un pequeño grupo de direcciones destino	Dirección destino, puerto destino
Escaneo de Red	Prueba diferentes direcciones de red de un grupo pequeño de puertos destino	Dirección destino, puerto destino
Outage Events	Cambios de tráfico debido a fallos en el equipamiento o a mantenimiento	Principalmente las direcciones
Punto a multipunto	Tráfico de una sola fuente a muchas direcciones	Dirección origen y destino
Gusanos	Escaneo por gusanos a Hosts vulnerables	Dirección destino y puerto

- Detección: Método métricas volumen y Entropía

Mining Anomalies using Traffic Features Distributions

Procedimiento

- Estadísticas realizadas cada 5 minutos
- 3 Semanas de datos (Links de Abilene y Géant)
- Se trabaja con flujos Origen-Destino



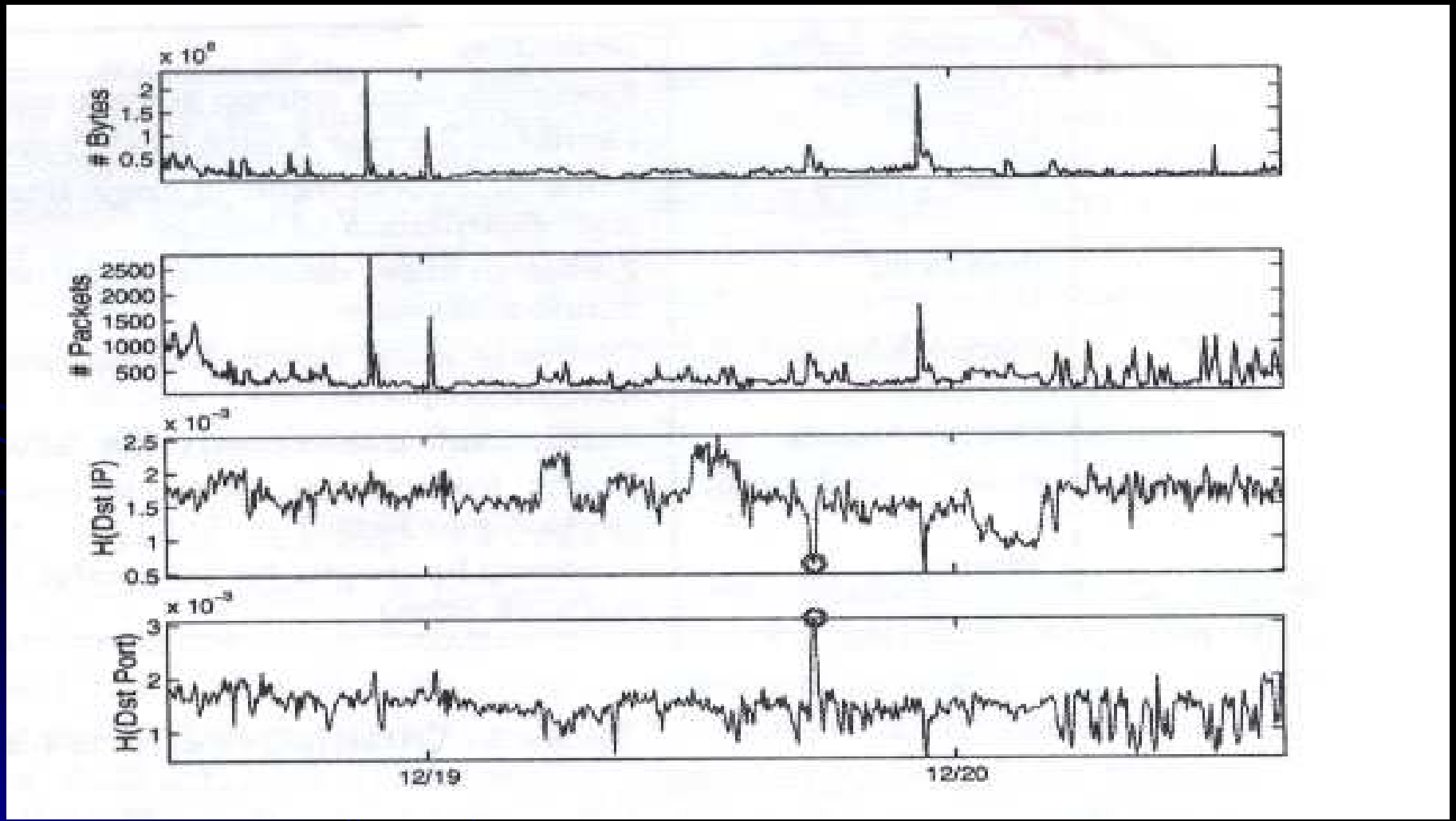
Mining Anomalies using Traffic Features Distributions

Procedimiento

- Se compara las anomalías obtenidas por técnicas de volumen y entropía.
  - Detección de anomalías de volumen: Se aplica el método del subespacio a flujos.
    - Número de Bytes
    - Número de Paquetes
  - Métrica de la ENTROPÍA: Método del subespacio multicamino
    - Dirección origen (srcIP)
    - Dirección destino (dstIP)
    - Puerto origen (srcPort)
    - Puerto destino (dstPort)

Mining Anomalies using Traffic Features Distributions

Procedimiento



Mining Anomalies using Traffic Features Distributions

Procedimiento

- Inspección manual de las anomalías y etiquetado.
- Ventajas Entropía:
  - Detecta anomalías no detectadas por el método del volumen
  - Porcentaje bajo de falsas alarmas.
- Aplicar algoritmos de Clustering para reconocer las anomalías.

Mining Anomalies using Traffic Features Distributions

Procedimiento

- Cada anomalía: H(srcIP),H(dstIP),H(srcPort),H(dstPort)
- Se reescala ||H||
- Algoritmos: K-means y Jerárquico.

- El número de Clusters es fijado a 10
- Se etiqueta cada Cluster comprobándose las características de cada anomalía.

Índice

- Introducción
- Anomaly Detection in IP Networks
- Mining Anomalies Using Traffic Feature Distributions
- Otros trabajos
- Conclusiones

Otros trabajos

- Learning Rules for Anomaly Detection of Hostile Network Traffic
  - Utiliza conexiones TCP
  - Aprende reglas según un antecedente
    - If port=80 and word3=HTTP/1.0 then word1=GET or POST
    - Algoritmo LERAD:
      - Genera reglas: Subconjunto aleatorio de una muestra S
      - Descartar reglas
      - Paso de entrenamiento 2: Escribir el consecuente para cada regla.
      - Validación
      - Test

Otros trabajos

- Anomaly Detection Based on Unsupervised Niche Clustering with Application to Network Intrusion Detection
  - UNC determina el número de clusters automáticamente
  - Utiliza Data Set: 10% KDDCup'99
    - Flujos
    - 42 Atributos
    - Contenía 22 tipos de ataques, 4 clases de intrusiones (U2R, R2L, DOS, PRB)

Índice

- Introducción
- Anomaly Detection in IP Networks
- Mining Anomalies Using Traffic Feature Distributions
- Otros trabajos
- Conclusiones

Conclusiones

- El estudio se realiza a nivel:
  - Flujo Origen-Destino
  - Conexiones TCP
- Las anomalías son previamente etiquetadas
- Uso de técnicas de Clustering para la clasificación

¿Alguna Pregunta?